(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-248232
(P2004-248232A)
(43)公開日　平成16年9月2日(2004.9.2)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601B	5J104
	H04L	9/00	601E	

審査請求 未請求　請求項の数 18　OL　（全 33 頁）

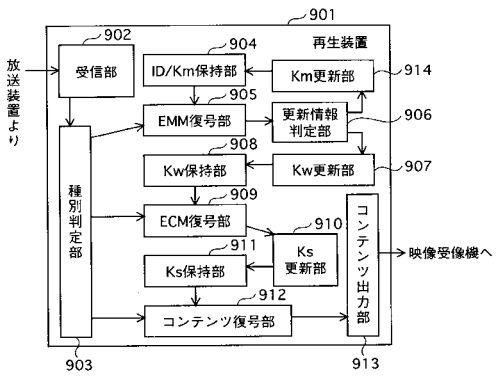
(21)出願番号　特願2003-54134(P2003-54134)
(22)出願日　平成15年2月28日(2003.2.28)
(31)優先権主張番号　特願2002-78397(P2002-78397)
(32)優先日　平成14年3月20日(2002.3.20)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願2002-364389(P2002-364389)
(32)優先日　平成14年12月16日(2002.12.16)
(33)優先権主張国　日本国(JP)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100090446
弁理士　中島　司朗
(72)発明者　小野　貴敏
愛知県名古屋市中区栄２丁目６番１号　白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内
(72)発明者　熊崎　洋児
愛知県名古屋市中区栄２丁目６番１号　白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内

最終頁に続く

(54)【発明の名称】コンテンツを再生する再生装置、再生方法、プログラム、鍵管理装置及び鍵管理システム

(57)【要約】
【課題】本発明は、不正な再生装置によるコンテンツの再生を排除し、正当な再生装置のみがコンテンツを適正に再生することができる技術を提供する。
【解決手段】本発明に係る再生装置は、秘密鍵を保持し（９０４）、秘密鍵暗号方式により暗号化された暗号化鍵情報を取得し（９０２、９０３）、秘密鍵を用いて暗号化鍵情報を復号して鍵情報を得る（９０５）。鍵情報が鍵更新情報であれば、鍵更新情報に基づいて秘密鍵を更新する（９１４）。鍵情報が復号鍵であれば、秘密鍵暗号方式により暗号化された暗号化コンテンツ鍵を取得して、復号鍵を用いて復号してコンテンツ鍵を得て（９１０）、スクランブル暗号方式によりスクランブルされたコンテンツを取得して、コンテンツ鍵を用いてデスクランブルして（９１２）コンテンツを再生する（９１３）。
【選択図】　図９



【特許請求の範囲】
【請求項１】
コンテンツを再生する再生装置であって、
秘密鍵を保持している保持手段と、
秘密鍵暗号方式により暗号化された暗号化鍵情報を取得し、前記保持手段により保持されている秘密鍵を用いて前記暗号化鍵情報を復号して鍵情報を得る鍵情報復号手段と、
前記鍵情報復号手段により得られた鍵情報が前記秘密鍵の更新に用いる鍵更新情報であるとき、当該鍵更新情報に基づいて新たな秘密鍵を生成し、前記鍵情報復号手段において用いる秘密鍵として、前記保持手段に保持させる生成手段と、
前記鍵情報復号手段により得られた鍵情報がコンテンツ鍵を復号するための復号鍵であるとき、秘密鍵暗号方式により暗号化された暗号化コンテンツ鍵を取得し、前記復号鍵を用いて復号してコンテンツ鍵を得て、スクランブル暗号方式によりスクランブルされたコンテンツを取得し、前記コンテンツ鍵を用いてデスクランブルしてコンテンツを再生するコンテンツ再生手段と
を備えることを特徴とする再生装置。
【請求項２】
前記鍵情報には、鍵更新情報であることを示す識別子又は復号鍵であることを示す識別子が付加されており、
前記再生装置は、さらに、
前記鍵情報復号手段により得られた鍵情報が、鍵更新情報であるか復号鍵であるかを識別子に基づいて判定する判定手段を備えること
を特徴とする請求項１に記載の再生装置。
【請求項３】
前記鍵情報は、ＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｍａｎａｇｅｍｅｎｔ　Ｍｅｓｓａｇｅｓ）に含まれており、
前記再生装置は、さらに、
前記秘密鍵により暗号化されたＥＭＭを含む放送データを受信し、暗号化された鍵情報を得る放送受信手段を備え、
前記鍵情報復号手段は、
前記放送受信手段により得られる暗号化された鍵情報を取得すること
を特徴とする請求項２に記載の再生装置。
【請求項４】
前記生成手段は、さらに、
再生装置毎、再生装置の生産ロット毎、再生装置の機種毎又は再生装置のメーカ毎に異なる所定の変換に基づいて新たな秘密鍵を生成すること
を特徴とする請求項１に記載の再生装置。
【請求項５】
前記鍵更新情報は、新たな秘密鍵の元となるシード情報を含み、
前記生成手段は、
前記シード情報に所定の変換を施して新たな秘密鍵を生成すること
を特徴とする請求項１に記載の再生装置。
【請求項６】
前記鍵更新情報は、秘密鍵の更新を指示するトリガ情報であり、
前記生成手段は、さらに、
前記トリガ情報に応じて前記秘密鍵を管理する鍵管理装置に秘密鍵の元となるシード情報の取得要求信号を送信する送信手段と、
前記取得要求信号に応じて前記鍵管理装置が送信するシード情報を受信するシード情報受信手段とを備え、
前記生成手段は、
前記シード情報受信手段により受信されたシード情報に所定の変換を施して新たな秘密鍵

を生成すること
を特徴とする請求項１に記載の再生装置。
【請求項７】
前記鍵更新情報は、新たな秘密鍵の元となるシード情報を含み、
前記生成手段は、さらに、
１回又は複数回ごとに異なるイベント情報を出力する出力手段を備え、
前記生成手段は、
所定の変換により、前記シード情報及び前記イベント情報に基づいて新たな秘密鍵を生成し、
前記再生装置は、さらに、
前記出力手段により出力された前記イベント情報を前記秘密鍵を管理する鍵管理装置に送信する送信手段を備えること
を特徴とする請求項１に記載の再生装置。
【請求項８】
前記保持手段は、
再生装置毎、再生装置の生産ロット毎、再生装置の機種毎又は再生装置のメーカ毎に個別の秘密鍵を保持していること
を特徴とする請求項１に記載の再生装置。
【請求項９】
前記再生装置は、再生装置毎、再生装置の生産ロット毎、再生装置の機種毎又は再生装置のメーカ毎に個別のＩＤを有し、
前記生成手段は、
前記シード情報及び前記ＩＤに所定の変換を施して新たな秘密鍵を生成すること
を特徴とする請求項１に記載の再生装置。
【請求項１０】
秘密鍵を保持する保持部を有する再生装置が、コンテンツを再生する再生方法であって、
秘密鍵暗号方式により暗号化された暗号化鍵情報を取得し、前記秘密鍵を用いて前記暗号化鍵情報を復号して鍵情報を得る鍵情報復号ステップと、
前記鍵情報復号ステップにより得られた鍵情報が前記秘密鍵の更新に用いる鍵更新情報であるとき、当該鍵更新情報に基づいて新たな秘密鍵を生成し、前記鍵情報復号ステップにおいて用いる秘密鍵として前記保持部に保持させる生成ステップと、
前記鍵情報復号ステップにより得られた鍵情報がコンテンツ鍵を復号するための復号鍵であるとき、秘密鍵暗号方式により暗号化された暗号化コンテンツ鍵を取得し、前記復号鍵を用いて復号してコンテンツ鍵を得て、スクランブル暗号方式によりスクランブルされたコンテンツを取得し、前記コンテンツ鍵を用いてデスクランブルしてコンテンツを再生するコンテンツ再生ステップと
を含むことを特徴とする再生方法。
【請求項１１】
秘密鍵の保持部を有するコンピュータにコンテンツを再生させるプログラムであって、
秘密鍵暗号方式により暗号化された暗号化鍵情報を取得し、前記秘密鍵を用いて前記暗号化鍵情報を復号して鍵情報を得る鍵情報復号ステップと、
前記鍵情報復号ステップにより得られた鍵情報が前記秘密鍵の更新に用いる鍵更新情報であるとき、当該鍵更新情報に基づいて新たな秘密鍵を生成し、前記鍵情報復号ステップにおいて用いる秘密鍵として前記保持部に保持させる生成ステップと、
前記鍵情報復号ステップにより得られた鍵情報がコンテンツ鍵を復号するための復号鍵であるとき、秘密鍵暗号方式により暗号化された暗号化コンテンツ鍵を取得し、前記復号鍵を用いて復号してコンテンツ鍵を得て、スクランブル暗号方式によりスクランブルされたコンテンツを取得し、前記コンテンツ鍵を用いてデスクランブルしてコンテンツを再生するコンテンツ再生ステップと
を含むことを特徴とするプログラム。

【請求項１２】
秘密鍵暗号方式における秘密鍵を管理する鍵管理装置であって、
前記秘密鍵の更新に用いる鍵更新情報を生成する鍵更新情報生成手段と、
前記生成手段により生成された鍵更新情報又はコンテンツを再生するための復号鍵を鍵情報とし、当該鍵情報を前記秘密鍵により暗号化して前記再生装置に送信する送信手段と、
前記鍵更新情報に基づいて新たな秘密鍵を生成し、前記送信手段において用いられる秘密鍵とする秘密鍵生成手段と
を備えることを特徴とする鍵管理装置。
【請求項１３】
前記送信手段は、さらに、
前記鍵情報に、当該鍵情報が鍵更新情報であることを示す識別子又は復号鍵であることを示す識別子を付加して送信すること
を特徴とする請求項１２に記載の鍵管理装置。
【請求項１４】
前記鍵情報は、ＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｍａｎａｇｅｍｅｎｔ Ｍｅｓｓａｇｅｓ）に含まれており、
前記送信手段は、
前記鍵情報を放送により再生装置に送信すること
を特徴とする請求項１３の鍵管理装置。
【請求項１５】
前記鍵更新情報は、新たな秘密鍵の元となるシード情報を含み、
前記秘密鍵生成手段は、
前記シード情報に所定の変換を施して新たな秘密鍵を生成すること
を特徴とする請求項１２に記載の鍵管理装置。
【請求項１６】
前記鍵更新情報は、秘密鍵の更新を指示するトリガ情報であり、
前記秘密鍵生成手段は、さらに、
新たな秘密鍵の元となるシード情報を生成するシード情報生成手段と、
前記トリガ情報を取得した再生装置から送信される取得要求信号を受信し、当該取得要求信号に応じて、前記シード情報生成手段により生成されたシード情報を前記再生装置に伝送する伝送手段とを含み、
前記秘密鍵生成手段は、
前記シード情報に所定の変換を施して新たな秘密鍵を生成すること
を特徴とする請求項１２に記載の鍵管理装置。
【請求項１７】
前記鍵更新情報は、新たな秘密鍵の元となるシード情報を含み、
前記秘密鍵生成手段は、さらに、
前記シード情報を取得した再生装置から送信される１回又は複数回ごとに異なるイベント情報を受信する受信手段を含み、
前記秘密鍵生成手段は、
所定の変換により、前記シード情報及び前記イベント情報に基づいて新たな秘密鍵を生成すること
を特徴とする請求項１２に記載の鍵管理装置。
【請求項１８】
コンテンツを再生する再生装置と、当該再生装置の秘密鍵暗号方式における秘密鍵を管理する鍵管理装置からなる鍵管理システムであって、
鍵管理装置において、前記秘密鍵の更新に用いる鍵更新情報を生成する鍵更新情報生成手段と、
前記鍵更新情報生成手段により生成された鍵更新情報又はコンテンツを再生するための復号鍵を鍵情報とし、当該鍵情報を前記秘密鍵により暗号化して前記再生装置に送信する送

信手段と、
前記再生装置において、前記送信手段により送信される暗号化鍵情報を取得し、保持している秘密鍵を用いて当該暗号化鍵情報を復号して前記鍵情報を得る鍵情報復号手段と、
前記鍵管理装置において、前記鍵更新情報に基づいて新たな秘密鍵を生成し、前記送信手段において用いる秘密鍵とする第１生成手段と、
前記再生装置において、前記鍵情報復号手段により復号された鍵情報が鍵更新情報であるとき、前記鍵更新情報に基づいて新たな秘密鍵を生成し、前記鍵情報復号手段において用いる秘密鍵とする第２生成手段と
を備えることを特徴とする鍵管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル放送においてコンテンツの視聴を許可されたユーザの再生装置のみが適正にコンテンツを再生することができる放送受信システム（以下、「限定受信システム」という。）に関する。特に、コンテンツの再生に必要なマスタ鍵を更新する技術に関する。

【０００２】

【従来の技術】

標準的な限定受信システムであるＭＰＥＧ２ＳＹＳＴＥＭＳ（ＩＳＯ／ＩＥＣ１３８１８－１）では、送信側は、映像や音声等のコンテンツをスクランブル鍵Ｋｓによりスクランブルしてから送信する。また受信側は、スクランブル鍵Ｋｓによりスクランブルを解いてコンテンツを再生する。このとき、送信側及び受信側は、同一のスクランブル鍵Ｋｓを保有していなければならない。

【０００３】

そのため、送信側は、スクランブル鍵ＫｓをＥＣＭ（ＥｎｔｉｔｌｅｍｅｎｔＣｏｎｔｒｏｌ　Ｍｅｓｓａｇｅｓ）と呼ばれる情報に格納し、ＥＣＭをワーク鍵Ｋｗで暗号化してから送信する。さらに、送信側は、ワーク鍵ＫｗをＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｍａｎａｇｅｍｅｎｔ　Ｍｅｓｓａｇｅｓ）と呼ばれる情報に格納し、ＥＭＭを再生装置ごとに固有のマスタ鍵Ｋｍで暗号化してから送信する。

【０００４】

受信側は、ＥＭＭを自己が有するマスタ鍵Ｋｍで復号化してワーク鍵Ｋｗを取得し、ＥＣＭをワーク鍵Ｋｗで復号化してスクランブル鍵Ｋｓを取得する。これにより、送信側及び受信側は、同一のスクランブル鍵Ｋｓを保有することができる。
図１は、限定受信システムの概略を示す図である。

【０００５】

放送装置１０１は、スクランブルされたコンテンツ、ＥＣＭ、ＥＭＭ等の各種情報を多重化して放送により再生装置１０２に送信する。再生装置１０２は、各種情報を復号して映像受像機１０３に表示する。ここで、再生装置１０２は、内部に保持しているＩＤとマスタ鍵Ｋｍとを用いてスクランブルを解いている。ＩＤは、再生装置ごと、あるいは、製造メーカごとなど必要に応じて割り振られている。また、マスタ鍵Ｋｍも、再生装置ごと、あるいは、製造メーカごとなど必要に応じて割り振られており、ＩＤと１対１で対応している。

【０００６】

図２は、限定受信システムにおける再生装置の構成を示す図である。
再生装置２０１は、受信部２０２でスクランブルされたコンテンツ、ＥＣＭ、ＥＭＭ等の各種情報を受信し、種別判定部２０３で各種情報の種別を判定する。種別判定部２０３は、情報がスクランブルされたコンテンツであればコンテンツ復号部２１１に、ＥＣＭであればＥＣＭ復号部２０８に、ＥＭＭであればＥＭＭ復号部２０５に転送する。

【０００７】

ＩＤ／Ｋｍ保持部２０４は、再生装置２０１に固有のＩＤとマスタ鍵Ｋｍとを保持してい

る。また、ＥＭＭ復号部２０５は、マスタ鍵Ｋｍを用いてＥＭＭを復号し、復号されたＥＭＭの一部であるワーク鍵ＫｗをＫｗ更新部２０６に入力する。Ｋｗ更新部２０６は、ＥＭＭ復号部２０５からワーク鍵Ｋｗを取得し、従来のワーク鍵を更新する。Ｋｗ保持部２０７は、Ｋｗ更新部２０６が更新したワーク鍵Ｋｗを保持する。

【０００８】

なお、ワーク鍵Ｋｗを更新するために双方向通信を用いて新たなワーク鍵を取得する例もある（例えば、特許文献１参照）。

ＥＣＭ復号部２０８は、ワーク鍵Ｋｗを用いてＥＣＭを復号し、復号されたＥＣＭの一部であるスクランブル鍵ＫｓをＫｓ更新部２０９に入力する。Ｋｓ更新部２０９は、ＥＣＭ復号部２０８からスクランブル鍵Ｋｓを取得し、従来のスクランブル鍵を更新する。

【０００９】

なお、ワーク鍵の更新及びスクランブル鍵の更新は、通常上書きによる書き換えであるが、追加という形としてもよい。

Ｋｓ保持部２１０は、Ｋｓ更新部２０９が更新したスクランブル鍵Ｋｓを保持する。コンテンツ復号部２１１は、スクランブル鍵Ｋｓを用いてスクランブルされたコンテンツを復号し、復号されたコンテンツをコンテンツ出力部２１２に入力する。コンテンツ出力部２１２は、コンテンツを映像受像機に送信する。

【００１０】

図３は、限定受信システムにおける再生装置の動作を示す図である。

再生装置は、放送装置からのＥＭＭを受信する（Ｓ３０１）。ＥＭＭは、そのＥＭＭが受信されるべき再生装置のＩＤと、ワーク鍵ＫｗをＩＤに対応したマスタ鍵Ｋｍで暗号化した暗号化ワーク鍵Ｅ（Ｋｗ、Ｋｍ）とを含んでいる。（ここで、Ｅ（Ｘ、Ｙ）は、情報Ｘを鍵Ｙで暗号化されたものを意味する。以下も同様とする。）

再生装置は、ＥＭＭに含まれているＩＤが自己の保持するＩＤと一致すれば、保持しているＫｍを用いてＥ（Ｋｗ、Ｋｍ）を復号する。その結果、再生装置は、ワーク鍵Ｋｗを取得することができる（Ｓ３０２）。

【００１１】

さらに、再生装置は、放送装置からのＥＣＭを受信する（Ｓ３０３）。ＥＣＭは、スクランブル鍵Ｋｓをワーク鍵Ｋｗで暗号化した暗号化スクランブル鍵Ｅ（Ｋｓ、Ｋｗ）を含んでいる。

再生装置は、保持しているワーク鍵Ｋｗを用いてＥ（Ｋｓ、Ｋｗ）を復号する。その結果、再生装置は、スクランブル鍵Ｋｓを取得することができる（Ｓ３０４）。

【００１２】

さらに、再生装置は、放送装置からのスクランブルされたコンテンツＥ（Ｃｏｎｔｅｎｔ、Ｋｓ）を受信する（Ｓ３０５）。

再生装置は、保持しているスクランブル鍵Ｋｓを用いてＥ（Ｃｏｎｔｅｎｔ、Ｋｓ）を復号する。その結果、再生装置はコンテンツを取得することができる（Ｓ３０６）。これによりユーザは、コンテンツを視聴することができる。

【００１３】

図４は、複数の再生装置における限定受信システムの概略を示す図である。

再生装置１及び再生装置２は、放送装置１０１から送信された各種情報を受信する。なお映像受像機については省略している。ＩＤ１及びＩＤ２は、再生装置ごとに割り振られており、互いに異なる。また、ＩＤとマスタ鍵Ｋｍとは１対１に対応しているので、Ｋｍ１及びＫｍ２も互いに異なる。なお、ここではＩＤを再生装置ごとに割り振っているが、例えば製造メーカごと、再生装置機種ごと、生産ロットごと等、特定のグループごとに割り振ってもよい。その場合、グループ内の複数の再生装置が同じＩＤとマスタ鍵Ｋｍを保持することになるが、別のグループの再生装置が保持するＩＤとマスタ鍵Ｋｍとは異なることになる。

【００１４】

図５は、限定受信システムにおける複数の再生装置の動作を示す図である。

再生装置１は、放送装置からのＥＭＭ１を選択的に受信する（Ｓ５０１）。ＥＭＭ１は、ＩＤ１と、ワーク鍵ＫｗをＩＤ１に対応したマスタ鍵Ｋｍ１で暗号化した暗号化ワーク鍵Ｅ（Ｋｗ、Ｋｍ１）とを含んでいる。そのため、再生装置１は、ＥＭＭ１のＩＤ１により、このＥＭＭが自己宛のＥＭＭであると認識することができる。

【００１５】

再生装置１は、保持しているＫｍ１を用いてＥ（Ｋｗ、Ｋｍ１）を復号する。これにより、再生装置１はワーク鍵Ｋｗを取得することができる（Ｓ５０２）。

再生装置２は、放送装置からのＥＭＭ２を選択的に受信する（Ｓ５０３）。ＥＭＭ２は、ＩＤ２と、ワーク鍵ＫｗをＩＤ２に対応したマスタ鍵Ｋｍ２で暗号化した暗号化ワーク鍵Ｅ（Ｋｗ、Ｋｍ２）とを含んでいる。そのため、再生装置２は、ＥＭＭ２のＩＤ２により、このＥＭＭが自己宛のＥＭＭであると認識することができる。

【００１６】

再生装置２は、保持しているＫｍ２を用いてＥ（Ｋｗ、Ｋｍ２）を復号する。これにより、再生装置２はワーク鍵Ｋｗを取得することができる（Ｓ５０４）。

このように、再生装置１及び再生装置２はそれぞれワーク鍵Ｋｗを取得する。その後の手順は、図３と同様なので説明を省略する。

次に、不正再生装置が存在する場合に、不正再生装置によるコンテンツの再生を阻止する方法を示す。

【００１７】

図６は、不正再生装置が存在する場合の限定受信システムの概略を示す図である。

不正再生装置は、不正にＩＤ２とマスタ鍵Ｋｍ２とを取得して、再生装置２になりすます再生装置である。このような状態であれば、図５で示した動作と同じ手順によって、不正再生装置は、あたかも自己が再生装置２であるかのように振るまい、コンテンツを再生することができる。

【００１８】

そこで、不正再生装置の存在が発覚したとき、コンテンツの不正な再生を阻止するべく、放送装置がＩＤ２を含むＥＭＭを送信しない方法が考えられる。

図７は、不正再生装置によるコンテンツの不正な再生を阻止する場合の各再生装置の動作を示す図である。

図５と異なるのは、放送装置が再生装置１向けのＥＭＭ１のみを送信し（Ｓ５０１）、再生装置２向けのＥＭＭ２を送信しないことにある。これにより、不正再生装置は、ワーク鍵Ｋｗを取得することができない。したがって、不正再生装置は、スクランブル鍵Ｋｓを取得することができず（Ｓ７０１）、コンテンツを受信することができない（Ｓ７０２）。

【００１９】

【特許文献１】

特開２００２－１６９０１号公報

【００２０】

【発明が解決しようとする課題】

しかしながら、放送装置がＩＤ２を含むＥＭＭを送信しない方法によれば、正当な再生装置２までもがコンテンツを再生できないという問題が生じる。

そこで、本発明は、不正再生装置によるコンテンツの再生を排除し、正当な再生装置のみがコンテンツを適正に再生することができる技術を提供することを第１の目的とする。さらに、コンテンツが送信されるチャンネルを有効利用して、正当な再生装置のみがコンテンツを適当に再生することができる技術を提供することを第２の目的とする。

【００２１】

【課題を解決するための手段】

上記目的を達成するために、本発明に係るコンテンツを再生する再生装置は、秘密鍵を保持している保持手段と、秘密鍵暗号方式により暗号化された暗号化鍵情報を取得し、前記保持手段により保持されている秘密鍵を用いて前記暗号化鍵情報を復号して鍵情報を得る

鍵情報復号手段と、前記鍵情報復号手段により得られた鍵情報が前記秘密鍵の更新に用いる鍵更新情報であるとき、当該鍵更新情報に基づいて新たな秘密鍵を生成し、前記鍵情報復号手段において用いる秘密鍵として、前記保持手段に保持させる生成手段と、前記鍵情報復号手段により得られた鍵情報がコンテンツ鍵を復号するための復号鍵であるとき、秘密鍵暗号方式により暗号化された暗号化コンテンツ鍵を取得し、前記復号鍵を用いて復号してコンテンツ鍵を得て、スクランブル暗号方式によりスクランブルされたコンテンツを取得し、前記コンテンツ鍵を用いてデスクランブルしてコンテンツを再生するコンテンツ再生手段とを備えることを特徴とする。

【００２２】

上記構成によれば、再生装置は、鍵情報を取得し、鍵情報が鍵更新情報であるとき新たな秘密鍵を生成し、鍵情報が復号鍵であるとき当該復号鍵を用いてコンテンツの再生を行う。このように、鍵更新情報に基づいて新たな秘密鍵を生成することで、次回から新たな秘密鍵により暗号化された鍵情報を適正に復号することができる。

【００２３】

したがって、秘密鍵の更新後は、正当な再生装置のみがコンテンツを再生でき、不正な再生装置によるコンテンツの再生を排除することができる。

【００２４】

【発明の実施の形態】

（実施の形態１）

［限定受信システムの概要］

図８は、本実施の形態における限定受信システムの概要を示す図である。

本実施の形態における限定受信システムは、鍵管理装置８０１、製造装置８０２、再生装置８０３及び放送装置８０４からなる。

【００２５】

まず最初に、鍵管理装置８０１と再生装置８０３とが同一のＩＤとマスタ鍵Ｋｍとを保有する手順を示す。

鍵管理装置８０１は、再生装置ごと、生産ロットごと、機種ごと、製造メーカごとなど必要に応じて固有のＩＤとマスタ鍵Ｋｍとを割り振り、それらを製造装置８０２に提供する。

【００２６】

再生装置８０３を製造する製造装置８０２は、鍵管理装置８０１から割り振られたＩＤとマスタ鍵Ｋｍとを再生装置８０３に組み込んだ後に、その再生装置８０３をユーザに提供する。

このようにして、鍵管理装置８０１と再生装置８０３とは、同一のＩＤとマスタ鍵Ｋｍとを保有することができる。

【００２７】

次に、ユーザが所望のコンテンツを視聴する場合の手順を示す。ここで具体例として、ユーザの再生装置８０３は、ＩＤ「００００００００１」、マスタ鍵Ｋｍ「２７８３２５２９」が格納されているとする。

ユーザは、所望のコンテンツを放送している放送装置８０４に、コンテンツの視聴を申し込む。この際に、自己の再生装置８０３に格納されているＩＤ「００００００００１」を放送装置８０４に通知する。

【００２８】

放送装置８０４は、ユーザからの申し込みを受けて、再生装置８０３のＩＤ「００００００００１」とワーク鍵ＫｗとをＥＭＭに格納し、鍵管理装置８０１に送信する。

ここで、ワーク鍵Ｋｗは、視聴を許可されたユーザの再生装置のみが得られる鍵である。

【００２９】

鍵管理装置８０１は、放送装置８０４からＥＭＭを受信して、そのＥＭＭに格納されているＩＤ「００００００００１」を抽出する。そして、そのＩＤに対応するマスタ鍵Ｋｍ「２７８３２５２９」を特定し、ＥＭＭをマスタ鍵Ｋｍ「２７８３２５２９」により暗号化し

て放送装置８０４に送信する。
放送装置８０４は、暗号化されたＥＭＭを放送する。
【００３０】
再生装置８０３は、ＥＭＭを受信して、ＥＭＭに格納されているＩＤにより、そのＥＭＭが自己宛に放送されたものであるか否か判定する。この場合、ＥＭＭに格納されているＩＤが「００００００００１」であるので、自己宛であると判定する。そして、再生装置８０３は、ＥＭＭをマスタ鍵Ｋｍ「２７８３２５２９」により復号化し、ワーク鍵Ｋｗを取得する。
【００３１】
このようにして、放送装置８０４と再生装置８０３とは、同一のワーク鍵Ｋｗを保有することができる。
また放送装置８０４は、ＥＭＭだけではなく、スクランブル鍵Ｋｓを含むＥＣＭやスクランブル鍵Ｋｓによりスクランブルされたコンテンツなどを放送している。ユーザの再生装置８０３は、ワーク鍵ＫｗによりＥＣＭを復号化することでスクランブル鍵Ｋｓを取得し、スクランブル鍵Ｋｓによりスクランブルされたコンテンツを復号化することでコンテンツを取得することができる。
【００３２】
次に、本実施の形態の特徴であるマスタ鍵Ｋｍの更新について説明する。
マスタ鍵Ｋｍは、原則として更新する必要はない。しかし、例えば再生装置８０３のＩＤ「００００００００１」とマスタ鍵Ｋｍ「２７８３２５２９」とが他のユーザに漏洩したとき、他のユーザは、そのＩＤとマスタ鍵Ｋｍとを自己の再生装置にコピーして登録することで、再生装置８０３のユーザが視聴することを許可されたコンテンツを、不正に視聴することができる。このようなときにマスタ鍵Ｋｍを更新する必要性がでてくる。
【００３３】
このような場合、放送装置８０４が、更新をするべき再生装置のＩＤと新たなマスタ鍵の元となるシード情報とをＥＭＭに格納して放送する。そして、更新をするべき再生装置が、シード情報により新たなマスタ鍵を生成する。
ここで、シード情報から新たなマスタ鍵を生成するアルゴリズムは、再生装置の製造時に定められ、セキュリティの確保された状態で再生装置に組み込まれている。また、同じアルゴリズムが、鍵管理装置においてもセキュリティの確保された状態で組み込まれている。即ち、アルゴリズムは、鍵管理装置と正当なユーザの再生装置のみが同一のものを保有しているので、鍵管理装置と正当なユーザの再生装置とだけが同一の新たなマスタ鍵を保有することができる。
【００３４】
したがって、本実施の形態に係る限定受信システムは、マスタ鍵の更新後において、他のユーザによるコンテンツの不正な視聴を排除することができる。
このような限定受信システムを実現する再生装置及び鍵管理装置について以下に詳細に説明する。
［再生装置の構成］
図９は、限定受信システムにおける再生装置の構成を示す図である。
【００３５】
再生装置９０１は、受信部９０２、種別判定部９０３、ＩＤ／Ｋｍ保持部９０４、ＥＭＭ復号部９０５、更新情報判定部９０６、Ｋｗ更新部９０７、Ｋｗ保持部９０８、ＥＣＭ復号部９０９、Ｋｓ更新部９１０、Ｋｓ保持部９１１、コンテンツ復号部９１２、コンテンツ出力部９１３及びＫｍ更新部９１４を備える。
受信部９０２は、スクランブルされたコンテンツ、ＥＣＭ、ＥＭＭ等の各種情報を放送装置から受信する。
【００３６】
種別判定部９０３は、各種情報の種別を判定して各復号部に転送する。これにより、スクランブルされたコンテンツはコンテンツ復号部９１２に、ＥＣＭはＥＣＭ復号部９０９に

、ＥＭＭはＥＭＭ復号部９０５に転送される。
ＩＤ／Ｋｍ保持部９０４は、再生装置９０１に固有のＩＤとマスタ鍵Ｋｍとを保持しており、必要に応じてＥＭＭ復号部９０５にマスタ鍵Ｋｍを入力する。なお、マスタ鍵Ｋｍは、製造メーカにより組み込まれたものを初期値とし、その後必要に応じてＫｍ更新部９１４により更新される。

【００３７】

ＥＭＭ復号部９０５は、マスタ鍵Ｋｍを用いてＥＭＭを復号して、更新情報判定部９０６に入力する。
更新情報判定部９０６は、ＥＭＭに含まれる識別子によりそのＥＭＭがマスタ鍵Ｋｍの更新のためにシード情報を含むか、ワーク鍵Ｋｗの更新のために新たなワーク鍵Ｋｗを含むかを判定する。なお、識別子に関しては、後に説明する。

【００３８】

更新情報判定部９０６は、ワーク鍵Ｋｗが格納されていれば、そのワーク鍵ＫｗをＫｗ更新部９０７に入力する。シード情報が格納されていれば、そのシード情報をＫｍ更新部９１４に入力する。
Ｋｗ更新部９０７は、更新情報判定部９０６からワーク鍵Ｋｗを取得し、ワーク鍵を更新する。ワーク鍵の更新は、通常上書きによる書き換えであるが、追加という形としてもよい。

【００３９】

Ｋｗ保持部９０８は、Ｋｗ更新部９０７が更新したワーク鍵Ｋｗを保持し、必要に応じてＥＣＭ復号部９０９にワーク鍵Ｋｗを入力する。
ＥＣＭ復号部９０９は、ワーク鍵Ｋｗを用いてＥＣＭを復号し、ＥＣＭに格納されているスクランブル鍵ＫｓをＫｓ更新部９１０に入力する。
Ｋｓ更新部９１０は、ＥＣＭ復号部９０９からスクランブル鍵Ｋｓを取得し、スクランブル鍵を更新する。スクランブル鍵の更新は、通常上書きによる書き換えであるが、追加という形としてもよい。

【００４０】

Ｋｓ保持部９１１は、Ｋｓ更新部９１０が更新したスクランブル鍵Ｋｓを保持し、必要に応じてコンテンツ復号部９１２にスクランブル鍵Ｋｓを入力する。
コンテンツ復号部９１２は、スクランブル鍵Ｋｓを用いてスクランブルされたコンテンツを復号し、復号されたコンテンツをコンテンツ出力部９１３に入力する。

【００４１】

コンテンツ出力部９１３は、コンテンツを映像受像機に送信する。
Ｋｍ更新部９１４は、更新情報判定部９０６からシード情報を取得し、シード情報を用いてマスタ鍵Ｋｍを更新する。マスタ鍵の更新は、通常上書きによる書き換えであるが、追加という形としてもよい。これにより、ＩＤ／Ｋｍ保持部９０４は、最新のマスタ鍵以外に、更新前のマスタ鍵も保持されるので、最新のマスタ鍵が何らかの不具合により使用できなくなったときに、更新前のいずれかのマスタ鍵を用いることができる。また、ＩＤ／Ｋｍ保持部９０４は、最新のマスタ鍵以外に、初期状態のマスタ鍵のみを保持していてもよい。

【００４２】

また、マスタ鍵の更新と共にＩＤの更新を行ってもよいし、ＩＤの一部を世代番号として使用して、ＩＤとマスタ鍵との組み合わせが世代更新されていくこととしてもよい。このときＩＤの更新は、上書きによる書き換えとしてもよいし、追加という形としてもよい。
図１０は、実施の形態１におけるＫｍ更新部の詳細な構成を示す図である。

【００４３】

Ｋｍ更新部９１４は、シード情報取得部１００１、Ｋｍ生成部１００２及びＫｍ保存部１００３からなる。
シード情報取得部１００１は、更新情報判定部からシード情報を取得し、シード情報をＫｍ生成部１００２のマスタ鍵生成アルゴリズムの引数として入力する。

【００４４】
Ｋｍ生成部１００２は、組み込まれているアルゴリズムにより新たなマスタ鍵Ｋｍ’を生成する。なお、このアルゴリズムは、再生装置ごと、生産ロットごと、機種ごと、あるいは製造メーカごとに異なり、同一のものが鍵管理装置においても保有されている。
Ｋｍ保存部１００３は、ＩＤ／Ｋｍ保持部９０４が保持できる形でマスタ鍵Ｋｍを保存する。
【００４５】
このように、再生装置９０１は、放送装置から放送されるＥＭＭを用いてマスタ鍵Ｋｍを更新することができる。
なお、Ｋｍ更新部において、新たなマスタ鍵の生成のタイミングにより以下の２通りの方法に分けられるが、どちらを採用してもよい。
第１の方法は、シード情報を取得すればすぐに新たなマスタ鍵の生成処理を行う方法である。
【００４６】
第２の方法は、シード情報を取得してからそのままシード情報を保持しておき、必要に応じて新たなマスタ鍵の生成処理を行う方法である。この場合、例えば、ＥＭＭ復号部にＥＭＭが入力されたときに、ＥＭＭ復号部から信号を受けてから新たなマスタ鍵の生成処理を開始するなどが考えられる。
次に、ＥＭＭのデータ構造について説明する。
【００４７】
図１１は、通常のＥＭＭのデータ構造を示す図である。
ＥＭＭは、ＩＤ部とデータ部とからなる。ＩＤ部は、このＥＭＭを受信するべき再生装置のＩＤが格納される。これにより、再生装置は、放送装置から放送されるＥＭＭのうち、自己のＩＤが格納されたＥＭＭのみを選択的に復号することができる。
【００４８】
また、データ部は、識別子と鍵情報とが格納される。識別子は、データ部に含まれている鍵情報がワーク鍵であるかシード情報であるかを識別するための情報であり、例えば「０ｘ０１」のとき、ワーク鍵Ｋｗが含まれており、「０ｘ０２」のとき、シード情報が含まれているなどとする。
その他、データ部には、情報長、プロトコル番号や有効期限なども格納されるが、これらについては説明を省略する。
【００４９】
図１２は、マスタ鍵Ｋｍの更新のためのＥＭＭのデータ構造を示す図である。
このＥＭＭは、通常のＥＭＭと同様にＩＤ部とデータ部とからなる。
データ部は、識別子とシード情報が格納されている。
シード情報は、新たなマスタ鍵の元となる情報であり、例えば、マスタ鍵Ｋｍの世代を表す世代番号や乱数など、あるいはそれらの組み合わせなどが考えられる。
【００５０】
図１３は、Ｋｍ生成部におけるアルゴリズムの例を示す図である。
（ａ）は、再生装置のＩＤと世代番号とからオリジナルハッシュ関数を用いてマスタ鍵Ｋｍを取得する方法を示す。
（ｂ）は、鍵管理装置で発生させた乱数からオリジナル暗号関数を用いて暗号化することでマスタ鍵Ｋｍを取得する方法を示す。
【００５１】
なお、新たなマスタ鍵を生成する方法としては、新たなマスタ鍵を安全に再生装置と鍵管理装置とで保有できれば上述したものに限らない。例えば、ＩＤ、世代番号、シード情報を製造メーカごとのオリジナルハッシュ関数に入力して生成する形でもよい。
［再生装置の動作］
図１４は、限定受信システムにおける再生装置の動作を示す図である。
【００５２】

再生装置は、スクランブルされたコンテンツ、ＥＣＭ、ＥＭＭ等の各種情報を放送装置から受信する。ここでは、ＥＭＭを受信した場合のみを説明する。
再生装置がＥＭＭを受信すれば、そのＥＭＭに識別子によりワーク鍵が含まれているかシード情報が含まれているかを判定する（Ｓ１４０１）。
ＥＭＭにシード情報が含まれていれば（Ｓ１４０２、Ｙ）、再生装置は、ＥＭＭに含まれているシード情報を取得する（Ｓ１４０３）。

【００５３】

再生装置は、シード情報を元に新たなマスタ鍵を生成する（Ｓ１４０４）。
再生装置は、ステップＳ１４０４において生成したマスタ鍵を保持し、次回からは、そのマスタ鍵を使用する（Ｓ１４０５）。
ステップＳ１４０２において、ＥＭＭにワーク鍵が含まれていれば（Ｓ１４０２、Ｎ）、再生装置は、ワーク鍵を取得する（Ｓ１４０６）。

【００５４】

再生装置は、ステップＳ１４０６において復号したワーク鍵を保持し、次のＥＣＭの受信からは、そのワーク鍵を使用する（Ｓ１４０７）。
以上、ＥＭＭに格納されたシード情報により新たなマスタ鍵を生成することができる再生装置の構成及び動作について説明した。次に、再生装置と同一の新たなマスタ鍵を保有することができる鍵管理装置について説明する。
［鍵管理装置の構成］
図１５は、限定受信システムにおける鍵管理装置の構成を示す図である。

【００５５】

鍵管理装置１５０１は、ＥＭＭ受信部１５０２、鍵更新判定部１５０３、シード情報生成挿入部１５０４、Ｋｍ更新部１５０５、ＩＤ／Ｋｍ保持部１５０６、ＥＭＭ暗号部１５０７及び暗号化ＥＭＭ送信部１５０８からなる。
ＥＭＭ受信部１５０２は、放送装置から送信されたＥＭＭを受信して、鍵更新判定部１５０３に入力する。

【００５６】

鍵更新判定部１５０３は、ＥＭＭにマスタ鍵Ｋｍを更新すべきことを示す情報が格納されているか否か判定する。具体的には、識別子が「０ｘ０２」であるとき「マスタ鍵を更新すべきことを示す」と取り決めてあれば、その識別子が「０ｘ０２」であるか否か確認すればよい。識別子が「０ｘ０２」であれば、シード情報生成挿入部１５０４にその旨を通知する。なおＥＭＭは、ＥＭＭ暗号部１５０７に入力される。

【００５７】

シード情報生成挿入部１５０４は、鍵更新判定部１５０３からの通知を受けて、シード情報を生成してＥＭＭに挿入すると共に、そのシード情報をＫｍ更新部１５０５に入力する。シード情報は、新たなマスタ鍵の元となる情報であり、例えば、マスタ鍵Ｋｍの世代を表す世代番号や乱数などが考えられる。
Ｋｍ更新部１５０５は、シード情報生成挿入部１５０４からシード情報を取得し、シード情報を用いてマスタ鍵Ｋｍを更新する。ここで、シード情報から新たなマスタ鍵を生成するアルゴリズムは、再生装置においても保有されている。

【００５８】

ＩＤ／Ｋｍ保持部１５０６は、再生装置ごと、生産ロットごと、機種ごと、製造メーカごとなどに固有のＩＤとマスタ鍵Ｋｍとを保持しており、必要に応じてＥＭＭ暗号部１５０７にマスタ鍵Ｋｍを入力する。なお、マスタ鍵Ｋｍは、製造時に書き込まれたものを初期値とし、その後必要に応じてＫｍ更新部１５０５により更新される。

【００５９】

ＥＭＭ暗号部１５０７は、マスタ鍵Ｋｍを用いてＥＭＭを暗号化して、暗号化ＥＭＭ送信部１５０８に入力する。
暗号化ＥＭＭ送信部１５０８は、暗号化ＥＭＭを放送装置に送信する。
なお、シード情報を送るＥＭＭは、更新前の古いマスタ鍵により暗号化される。更新され

た新しいマスタ鍵により暗号化されるのは、次に送信されるＥＭＭからとなる。
【００６０】
このように、鍵管理装置は、シード情報を生成してＥＭＭに挿入し、そのシード情報を放送装置を通じて再生装置に送信すると共に、そのシード情報を元にマスタ鍵Ｋｍを更新する。一方、再生装置は、送信されたシード情報を元にマスタ鍵Ｋｍを更新する。ここで、鍵管理装置と再生装置とにおいて、シード情報からマスタ鍵を生成する同一のアルゴリズムが保有されているので、新たなマスタ鍵も鍵管理装置と再生装置とにおいて同一のものが保有される。
【００６１】
図１６に、鍵管理装置におけるＩＤとマスタ鍵Ｋｍとの管理例を示す。
鍵管理装置は、ＩＤ／Ｋｍ保持部においてＩＤとマスタ鍵Ｋｍとを図１６に示すような管理表によって一括管理している。管理表は、縦にＩＤ、横にマスタ鍵Ｋｍの各世代が配置されている。
鍵管理装置が製造装置にＩＤとマスタ鍵を割り振るときに、ＩＤとマスタ鍵Ｋｍとがこの管理表に追加される。このとき、マスタ鍵は、第１世代の欄に追加される。そして、マスタ鍵が更新されるたびに、新たなマスタ鍵が第２世代、第３世代というように順に追加されていく。
【００６２】
このように、過去のマスタ鍵も全て保持されるのには次の理由がある。
例えば、同一機種には同一のＩＤが割り振られているとしたとき、１回の更新情報の送信で全ての再生装置がマスタ鍵の更新に成功するとは限らず、その場合、マスタ鍵の更新に失敗した再生装置のために過去のマスタ鍵を用いて暗号化した更新情報を送信しなければならないからである。
［鍵管理装置の動作］
図１７は、限定受信システムにおける鍵管理装置の動作を示す図である。
【００６３】
鍵管理装置は、放送装置からＥＭＭを受信すれば、そのＥＭＭの識別子により秘密鍵を更新すべきか否か判定する（Ｓ１７０１）。
マスタ鍵を更新すべきであれば（Ｓ１７０２、Ｙ）、鍵管理装置は、シード情報を生成して（Ｓ１７０３）、そのシード情報をＥＭＭに挿入する（Ｓ１７０４）。
【００６４】
鍵管理装置は、ＩＤ／Ｋｍ保持部に保持しているマスタ鍵を取得して（Ｓ１７０５）、マスタ鍵を用いてＥＭＭを暗号化する（Ｓ１７０６）。
その後、鍵管理装置は、暗号化ＥＭＭを放送装置に送信する（Ｓ１７０７）。
ステップＳ１７０７において暗号化ＥＭＭを放送装置に送信した後、鍵管理装置は、ステップＳ１７０３において生成したシード情報を元にマスタ鍵を生成する（Ｓ１７０８）。
【００６５】
鍵管理装置は、ステップＳ１７０８において生成したマスタ鍵を保持し、次回からは、そのマスタ鍵を使用する（Ｓ１７０９）。
ステップＳ１７０２において、マスタ鍵を更新すべきでなければ（Ｓ１７０２、Ｎ）、鍵管理装置は、ＩＤ／Ｋｍ保持部に保持しているマスタ鍵を取得して（Ｓ１７１０）、マスタ鍵を用いてＥＭＭを暗号化する（Ｓ１７１１）。
【００６６】
その後、鍵管理装置は、暗号化ＥＭＭを放送装置に送信する（Ｓ１７１２）。
［限定受信システムの動作］
次に、上述した再生装置と鍵管理装置とを含む限定受信システムの動作について説明する。本実施の形態は、正規の再生装置になりすました不正再生装置の存在が発覚したとき、不正再生装置によるコンテンツの視聴を排除する動作に特徴があるので、特にその場面について説明する。
【００６７】

図１８は、不正再生装置によるコンテンツの不正な視聴を排除するときの各再生装置の動作を示す図である。
再生装置１は、正規にコンテンツの視聴を許可されたユーザ１の所有物であり、ＩＤ１とマスタ鍵Ｋｍ１とを有する。同様に、再生装置２は、正規にコンテンツの視聴を許可されたユーザ２の所有物であり、ＩＤ２とマスタ鍵Ｋｍ２とを有するものとする。また、不正再生装置は、再生装置２になりすましており、ＩＤ２とマスタ鍵Ｋｍ２とを有する。
【００６８】
このような状況で、放送装置が不正再生装置の存在を知り、不正再生装置によるコンテンツの視聴を排除する手順を示す。
放送装置は、再生装置１に対してＥＭＭ１を送信する（Ｓ１８０１）。
ＥＭＭは、そのＥＭＭが受信されるべき再生装置のＩＤと、ワーク鍵Ｋｗをマスタ鍵Ｋｍで暗号化した暗号化ワーク鍵Ｅ（Ｋｗ、Ｋｍ）とを含んでいる。即ち、ＥＭＭ１は、ＩＤ１と暗号化ワーク鍵Ｅ（Ｋｗ、Ｋｍ１）とを含んでいる。
【００６９】
再生装置１は、ＥＭＭ１に含まれているＩＤ１により自己宛のＥＭＭであると判定し、保持しているＫｍ１を用いてＥ（Ｋｗ、Ｋｍ１）を復号する。その結果、再生装置１は、ワーク鍵Ｋｗを取得することができる（Ｓ１８０２）。
また、放送装置は、再生装置２に対してＥＭＭ２を送信する（Ｓ１８０３）。
ＥＭＭ２は、ＩＤ２と暗号化シード情報Ｅ（Ｓｅｅｄ、Ｋｍ２）とを含んでいる。ここで、暗号化シード情報Ｅ（Ｓｅｅｄ、Ｋｍ２）とは、マスタ鍵Ｋｍ２を用いてシード情報Ｓｅｅｄを暗号化したものである。
【００７０】
再生装置２は、ＥＭＭ２に含まれているＩＤ２により自己宛のＥＭＭであると判定し、保持しているＫｍ２を用いてＥ（Ｓｅｅｄ、Ｋｍ２）を復号する。その結果、再生装置２は、シード情報Ｓｅｅｄを取得することができる（Ｓ１８０４）。
また、不正再生装置も、ＥＭＭ２に含まれているＩＤ２により自己宛のＥＭＭであると判定し、保持しているＫｍ２を用いてＥ（Ｓｅｅｄ、Ｋｍ２）を復号する。その結果、不正再生装置は、シード情報Ｓｅｅｄを取得することができる（Ｓ１８０５）。
【００７１】
再生装置２は、シード情報Ｓｅｅｄを元に新たなマスタ鍵Ｋｍ２’を生成する（Ｓ１８０６）。シード情報Ｓｅｅｄからマスタ鍵Ｋｍ２’を生成するアルゴリズムは、再生装置ごと、生産ロットごと、機種ごと、あるいは製造メーカごとなど個別のものである。なお、このアルゴリズムは、鍵管理装置においても保有されているため、鍵管理装置においてもシード情報Ｓｅｅｄからマスタ鍵Ｋｍ２’を生成することができる。したがって、再生装置２と鍵管理装置との間で同一の新たなマスタ鍵Ｋｍ２’を保有することができる。
【００７２】
一方、不正再生装置は、シード情報Ｓｅｅｄからマスタ鍵Ｋｍ２’を生成するアルゴリズムを持っていないため、マスタ鍵Ｋｍ２’を生成することができない（Ｓ１８０７）。
放送装置は、再生装置２に対してＥＭＭ２’を送信する（Ｓ１８０８）。
ここで、ＥＭＭ２’は、ＩＤ２と暗号化ワーク鍵Ｅ（Ｋｗ、Ｋｍ２’）とを含んでいる。
【００７３】
再生装置２は、ＥＭＭ２に含まれているＩＤ２により自己宛のＥＭＭであると判定し、保持しているＫｍ２’を用いてＥ（Ｋｗ、Ｋｍ２’）を復号する。その結果、再生装置２は、ワーク鍵Ｋｗを取得することができる（Ｓ１８０９）。
一方、不正再生装置も、ＥＭＭ２に含まれているＩＤ２により自己宛のＥＭＭであると判定するが、マスタ鍵Ｋｍ２’を保持していないので、ワーク鍵Ｋｗを取得することができない（Ｓ１８１０）。
【００７４】
放送装置は、再生装置１及び再生装置２に対してＥＣＭを送信する（Ｓ１８１１）。
ＥＣＭは、スクランブル鍵Ｋｓをワーク鍵Ｋｗで暗号化した暗号化スクランブル鍵Ｅ（Ｋ

ｓ、Ｋｗ）を含んでいる。
再生装置１は、ＥＣＭを受信し、ステップＳ１８０２において取得したワーク鍵Ｋｗを用いてＥ（Ｋｓ、Ｋｗ）を復号する。その結果、再生装置１は、スクランブル鍵Ｋｓを取得することができる（Ｓ１８１２）。
【００７５】
再生装置２は、ＥＣＭを受信し、ステップＳ１８０９において取得したワーク鍵Ｋｗを用いてＥ（Ｋｓ、Ｋｗ）を復号する。その結果、再生装置２は、スクランブル鍵Ｋｓを取得することができる（Ｓ１８１３）。
一方、不正再生装置は、ステップＳ１８１０においてワーク鍵Ｋｗを取得できないので、スクランブル鍵Ｋｓも取得することができない（Ｓ１８１４）。
【００７６】
放送装置は、再生装置１及び再生装置２に対してスクランブルされたコンテンツを送信する（Ｓ１８１５）。
スクランブルされたコンテンツＥ（Ｃｏｎｔｅｎｔ、Ｋｓ）は、コンテンツをスクランブル鍵Ｋｓでスクランブルしたものである。
再生装置１は、ステップＳ１８１２において取得したスクランブル鍵Ｋｓを用いてＥ（Ｃｏｎｔｅｎｔ、Ｋｓ）を復号する。その結果、再生装置１は、コンテンツを取得することができる（Ｓ１８１６）。
【００７７】
再生装置２は、ステップＳ１８１３において取得したスクランブル鍵Ｋｓを用いてＥ（Ｃｏｎｔｅｎｔ、Ｋｓ）を復号する。その結果、再生装置２は、コンテンツを取得することができる（Ｓ１８１７）。
一方、不正再生装置は、ステップＳ１８１４においてスクランブル鍵Ｋｓを取得できないので、コンテンツも取得することができない（Ｓ１８１８）。
【００７８】
このように、放送装置は、正当な再生装置になりすました不正再生装置の存在が発覚したとき、鍵管理装置と再生装置とが保有している同一のマスタ鍵を更新することで、不正再生装置によるコンテンツの視聴を排除することができる。
また、本実施の形態は、放送により送信されるＥＭＭを用いてマスタ鍵を更新するため、ＩＣカードなどの可搬メディアを用いてマスタ鍵を更新する方法に比べて日数がかからない。したがって、正当なユーザは、可搬メディアが到着するまで視聴したいコンテンツを視聴できないという不利益を被ることがない。
【００７９】
さらに、ＩＤとマスタ鍵Ｋｍとが再生装置ごとに割り振られていたものではなく、生産ロットごと、機種ごと、製造メーカごとなどに割り振られていた場合であっても、鍵管理装置は、該当する全ての再生装置に可搬メディアを送付する費用などの負担を負う必要がない。
（実施の形態２）
［限定受信システムの概要］
図１９は、本実施の形態における限定受信システムの概要を示す図である。
【００８０】
本実施の形態における限定受信システムは、鍵管理装置１９０１、製造装置１９０２、再生装置１９０３及び放送装置１９０４からなる。
鍵管理装置１９０１と再生装置１９０３とが同一のＩＤとマスタ鍵Ｋｍとを保有する手順と、再生装置１９０３がワーク鍵Ｋｗを取得する手順とは、実施の形態１と同様である。
【００８１】
本実施の形態と実施の形態１とが異なるのは、マスタ鍵Ｋｍを更新する方法である。
本実施の形態は、次のようにマスタ鍵Ｋｍを更新する。
放送装置１９０４が、更新をするべき再生装置のＩＤ、マスタ鍵Ｋｍを更新すべきこと示すトリガ情報をＥＭＭに格納して放送する。そして、更新をするべき再生装置が、更新情

報によりマスタ鍵Ｋｍを更新すべきことを認識し、自己のＩＤなどの装置情報を鍵管理装置１９０１に送信する。鍵管理装置１９０１は、新たなマスタ鍵の元となるシード情報を再生装置に送信する。再生装置は、シード情報を用いてマスタ鍵Ｋｍを更新する。

【００８２】

ここで、シード情報から新たなマスタ鍵Ｋｍ’を生成するアルゴリズムは、鍵管理装置と正当なユーザのみが同一のものを保有しているので、鍵管理装置と正当なユーザの再生装置のみが同一の新たなマスタ鍵Ｋｍ’を保有することができる。したがって、本実施の形態に係る限定受信システムは、マスタ鍵の更新後において、他のユーザによる不正な視聴を排除することができる。

【００８３】

実施の形態１は、ＥＭＭにシード情報を格納して送信していた。これに対し、本実施の形態は、ＥＭＭに単なるマスタ鍵の更新を開始するためのトリガ情報を格納して送信し、シード情報はＥＭＭ以外の手段で送信される点が異なる。

このような限定受信システムを実現する再生装置について以下に詳細に説明する。

［再生装置の構成］

本実施の形態における再生装置は、Ｋｍ更新部のみが実施の形態１の再生装置と異なる。したがって、Ｋｍ更新部のみを説明し、他の構成についての説明は省略する。

【００８４】

図２０は、実施の形態２におけるＫｍ更新部の詳細な構成を示す図である。

Ｋｍ更新部は、装置情報保持部２００１、装置情報送信部２００２、シード情報受信部２００３、Ｋｍ生成部２００４及びＫｍ保存部２００５からなる。

装置情報保持部２００１は、例えばＩＤなどの再生装置に個別の装置情報を保持しており、更新情報判定部からの通知に応じて装置情報を装置情報送信部２００２に入力する。

【００８５】

装置情報送信部２００２は、装置情報保持部２００１の保持している装置情報をシード情報の取得要求信号として鍵管理装置に送信する。鍵管理装置は、装置情報を受信した場合に、シード情報を返信する。

シード情報受信部２００３は、シード情報を受信し、シード情報をＫｍ生成部２００４のマスタ鍵生成アルゴリズムの引数として入力する。ここで、装置情報及びシード情報は、電話回線を用いて伝送される。

【００８６】

Ｋｍ生成部２００４は、組み込まれているアルゴリズムにより新たなマスタ鍵Ｋｍ’を生成する。なお、このアルゴリズムは、再生装置ごと、生産ロットごと、機種ごと、あるいは製造メーカごとに異なり、鍵管理装置においても保有されている。

Ｋｍ保存部２００５は、マスタ鍵Ｋｍを保存する。

【００８７】

なお、本実施の形態においても、新たなマスタ鍵の生成のタイミングにより以下の２通りの方法に分けられるが、どちらを採用してもよい。

第１の方法は、シード情報を取得すればすぐに新たなマスタ鍵の生成処理を行う方法である。

第２の方法は、シード情報を取得してからそのままシード情報を保持しておき、必要に応じて新たなマスタ鍵の生成処理を行う方法である。この場合、例えば、ＥＭＭ復号部にＥＭＭが入力されたときに、ＥＭＭ復号部から信号を受けてから新たなマスタ鍵の生成処理を開始するなどが考えられる。

【００８８】

図２１は、マスタ鍵Ｋｍの更新のためのＥＭＭのデータ構造を示す図である。

本実施の形態において、データ部は、識別子が格納されており、この識別子そのものがトリガ情報となる。

［鍵管理装置の構成］

図２２は、限定受信システムにおける鍵管理装置の構成を示す図である。

【００８９】
鍵管理装置２２０１は、ＥＭＭ受信部２２０２、鍵更新判定部２２０３、シード情報生成部２２０４、Ｋｍ更新部２２０５、ＩＤ／Ｋｍ保持部２２０６、ＥＭＭ暗号部２２０７、暗号化ＥＭＭ送信部２２０８、装置情報受信部２２０９及びシード情報送信部２２１０からなる。
本実施の形態における鍵管理装置は、シード情報生成部２２０４、装置情報受信部２２０９及びシード情報送信部２２１０が実施の形態１の鍵管理装置と異なる。したがって、異なる構成のみを説明し、同じ構成についての説明は省略する。
【００９０】
シード情報生成部２２０４は、鍵更新判定部２２０３からの通知を受けて、シード情報を生成してＫｍ更新部２２０５に入力すると共に、そのシード情報をシード情報送信部２２１０に入力する。シード情報は、新たなマスタ鍵の元となる情報であり、例えば、マスタ鍵Ｋｍの世代を表す世代番号や乱数などが考えられる。
【００９１】
装置情報受信部２２０９は、再生装置からＩＤなどの装置情報を受信して、その装置情報によりどの再生装置から送信されたものか特定する。
シード情報送信部２２１０は、装置情報受信部２２０９において特定された再生装置にシード情報を送信する。
このように、本実施の形態における鍵管理装置は、再生装置からのシード情報の取得要求にしたがってシード情報を送信する。また、再生装置は、ＥＭＭに含まれるトリガ情報によりマスタ鍵を更新すべきことを知り、シード情報の取得要求を鍵管理装置に送信する。
【００９２】
これにより、再生装置及び鍵管理装置は、同じシード情報を有し、そのシード情報から同じアルゴリズムを用いてそれぞれ新たなマスタ鍵を生成する。
また、本実施の形態において、再生装置は、マスタ鍵の更新をする際に、必ず鍵管理装置と通信を行わなければならない。これにより、鍵管理装置は、不正な再生装置の元となった再生装置を特定することができる。
【００９３】
例えば、再生装置が自己のＩＤを取得要求信号として送信する仕様であれば、不正な再生装置が存在した場合、鍵管理装置には、同一のＩＤが複数回送信されてくることになる。これにより、鍵管理装置は、そのＩＤの再生装置が不正な再生装置の元となったと判断することができる。
なお、本実施の形態において装置情報及びシード情報は、電話回線を用いて送信されているが、これに限らずオフライン送付などでもよい。また、シード情報は、ＥＭＭを用いて送信されてもよい。
（実施の形態３）
［限定受信システムの概要］
図２３は、本実施の形態における限定受信システムの概要を示す図である。
【００９４】
本実施の形態における限定受信システムは、鍵管理装置２３０１、製造装置２３０２、再生装置２３０３及び放送装置２３０４からなる。
鍵管理装置２３０１と再生装置２３０３とが同一のＩＤとマスタ鍵Ｋｍとを保有する手順と、再生装置２３０３がワーク鍵Ｋｗを取得する手順とは、実施の形態１と同様である。
【００９５】
本実施の形態と実施の形態１とが異なるのは、マスタ鍵Ｋｍを更新する方法である。
本実施の形態は、次のようにマスタ鍵Ｋｍを更新する。
放送装置２３０４が、更新をするべき再生装置２３０３のＩＤと新たなマスタ鍵Ｋｍ’の元となるシード情報とをＥＭＭに格納して放送する。
【００９６】
そして、再生装置２３０３が、シード情報によりマスタ鍵を更新すべきことを認識し、イ

ベント情報を発生させて、シード情報及びイベント情報から新たなマスタ鍵Ｋｍ’を生成する。ここで、イベント情報とは、更新ごとに個別の値を持つ情報である。本実施の形態は、イベント情報として乱数を使用する。
再生装置２３０３は、さらに、自己のＩＤと乱数とを含む装置情報を鍵管理装置２３０１に送信する。鍵管理装置２３０１は、シード情報及び乱数を用いてマスタ鍵を更新する。
【００９７】
ここで、シード情報と乱数から新たなマスタ鍵Ｋｍ’を生成するアルゴリズムは、鍵管理装置と正当なユーザの再生装置のみが有するので、鍵管理装置と正当なユーザの再生装置のみが新たなマスタ鍵Ｋｍ’を取得することができる。
したがって、本実施の形態に係る限定受信システムは、マスタ鍵の更新後において、他のユーザによる不正な視聴を排除することができる。
【００９８】
このような限定受信システムを実現する再生装置について以下に詳細に説明する。
［再生装置の構成］
本実施の形態における再生装置は、Ｋｍ更新部のみが実施の形態１の再生装置と異なる。したがって、Ｋｍ更新部のみを説明し、他の構成についての説明は省略する。
【００９９】
図２４は、実施の形態３におけるＫｍ更新部の詳細な構成を示す図である。
Ｋｍ更新部は、シード情報取得部２４０１、装置情報生成部２４０２、Ｋｍ生成部２４０３、Ｋｍ保存部２４０４及び装置情報送信部２４０５からなる。
シード情報取得部２４０１は、更新情報判定部からシード情報を取得し、シード情報をＫｍ生成部２４０３のマスタ鍵生成アルゴリズムの引数として入力する。
【０１００】
装置情報生成部２４０２は、更新情報判定部からの通知に応じて乱数を発生させ、予め保持しているＩＤと組み合わせて再生装置に個別の装置情報を生成する。装置情報は、Ｋｍ生成部２４０３と装置情報送信部２４０５とに入力される。
Ｋｍ生成部２４０３は、組み込まれているアルゴリズムにより新たなマスタ鍵Ｋｍ’を生成する。なお、このアルゴリズムは、再生装置ごと、生産ロットごと、機種ごと、あるいは製造メーカごとに異なり、鍵管理装置においても保有されている。
【０１０１】
Ｋｍ保存部２４０４は、マスタ鍵Ｋｍを保存する。
装置情報送信部２４０５は、装置情報生成部２４０２からの装置情報を鍵管理装置に送信する。ここで、装置情報は、電話回線を用いて送信される。
なお、本実施の形態においても、新たなマスタ鍵の生成のタイミングにより以下の２通りの方法に分けられるが、どちらを採用してもよい。
【０１０２】
第１の方法は、シード情報を取得すればすぐに新たなマスタ鍵の生成処理を行う方法である。
第２の方法は、シード情報を取得してからそのままシード情報を保持しておき、必要に応じて新たなマスタ鍵の生成処理を行う方法である。この場合、例えば、ＥＭＭ復号部にＥＭＭが入力されたときに、ＥＭＭ復号部から信号を受けてから新たなマスタ鍵の生成処理を開始するなどが考えられる。
［鍵管理装置の構成］
図２５は、限定受信システムにおける鍵管理装置の構成を示す図である。
【０１０３】
本実施の形態における鍵管理装置は、装置情報受信部２５０５とＫｍ更新部２５０６とが実施の形態１の鍵管理装置と異なる。したがって、装置情報受信部のみを説明し、他の構成についての説明は省略する。
装置情報受信部２５０５は、再生装置からの装置情報を受信する。ここで、装置情報は、再生装置のＩＤと再生装置で発生した乱数とからなる。装置情報受信部２５０５は、ＩＤ

により装置情報がどの再生装置から送信されたものか特定する。
【０１０４】
Ｋｍ更新部２５０６は、シード情報生成挿入部２５０４において生成されたシード情報と、装置情報受信部２５０５において受信された乱数とを用いてマスタ鍵を更新する。
なお、新たなマスタ鍵は、再生装置が有するアルゴリズムと同じアルゴリズムを用いて生成される。
【０１０５】
このように、本実施の形態における鍵管理装置は、シード情報をＥＭＭに含めて再生装置に送信し、再生装置から乱数を受信する。また、再生装置は、ＥＭＭに含まれるシード情報によりマスタ鍵を更新すべきことを知り、そのときに発生させた乱数を鍵管理装置に送信する。
これにより、再生装置及び鍵管理装置は、同じシード情報と同じ乱数を取得し、そのシード情報と乱数とから同じアルゴリズムを用いてそれぞれ新たなマスタ鍵を生成する。
【０１０６】
また、本実施の形態において、再生装置は、マスタ鍵の更新をする際に、必ず鍵管理装置と通信を行わなければならない。これにより、鍵管理装置は、不正な再生装置の元となった再生装置を特定することができる。
例えば、再生装置が自己のＩＤを取得要求信号として送信する仕様であれば、不正な再生装置が存在した場合、鍵管理装置には、同一のＩＤが複数回送信されてくることになる。これにより、鍵管理装置は、そのＩＤの再生装置が不正な再生装置の元となったと判断することができる。
【０１０７】
なお、本実施の形態において装置情報は、電話回線を用いて送信されているが、これに限らずオフライン送付などでもよい。
なお、全ての実施の形態において、再生装置及び鍵管理装置は、マスタ鍵のみを更新しているが、マスタ鍵とともにＩＤも更新してもよい。マスタ鍵及びＩＤの更新は、上書きでもよいし、一部を保持しておりその一部の保持されたＩＤが有効であるとしてもよいし、全て保持しており全てのＩＤが有効であるとしてもよい。
【０１０８】
なお、全ての実施の形態において、新たなマスタ鍵を生成するアルゴリズムは、鍵管理装置が管理しているが、セキュリティの確保された状態を実現さえすれば、これに限らない。例えば、複数の製造メーカが存在し、各製造メーカが自ら製造した再生装置のアルゴリズムを管理する場合、アルゴリズムが複数に分散されて管理されるのでリスク分散の効果がある。
【０１０９】
なお、実施の形態１は、マスタ鍵の更新方法を限定受信システムの再生装置に適用しているが、ＳＤカード、ＤＶＤの再生装置などのように、各種情報を保護するためにＩＤに対応する鍵を持つ装置にも適用可能である。以下にＤＶＤの再生装置への適用例を説明する。
図２６は、ＤＶＤの再生装置の構成を示す図である。
【０１１０】
再生装置２６０１は、読取部２６０２、種別判定部２６０３、デバイス鍵保持部２６０４、メディア鍵復号部２６０５、更新情報判定部２６０６、コンテンツ鍵復号部２６０７、コンテンツ復号部２６０８及びコンテンツ再生部２６０９を備える。
ＤＶＤの各種情報は、読取部２６０２で読み取られ、種別判定部２６０３で種別毎に振り分けられる。
【０１１１】
メディア鍵復号部２６０５は、デバイス鍵保持部２６０４に保持しているデバイス鍵を用いてデータを復号して更新情報判定部２６０６に入力する。
更新情報判定部２６０６は、データに更新情報が含まれていれば、そのデータをデバイス

鍵更新部２６１０に入力し、更新情報が含まれていなければ、そのデータをコンテンツ鍵復号部２６０７に入力する。

【０１１２】

デバイス鍵更新部２６１０は、更新情報を用いて新たなデバイス鍵を生成して、デバイス鍵保持部２６０４に保持されているデバイス鍵を更新する。

このように、再生装置２６０１は、更新情報判定部２６０６とデバイス鍵更新部２６１０によりデバイス鍵を更新することができる。

【０１１３】

【発明の効果】

本発明に係るコンテンツを再生する再生装置は、秘密鍵を保持している保持手段と、秘密鍵暗号方式により暗号化された暗号化鍵情報を取得し、前記保持手段により保持されている秘密鍵を用いて前記暗号化鍵情報を復号して鍵情報を得る鍵情報復号手段と、前記鍵情報復号手段により得られた鍵情報が前記秘密鍵の更新に用いる鍵更新情報であるとき、当該鍵更新情報に基づいて新たな秘密鍵を生成し、前記鍵情報復号手段において用いる秘密鍵として、前記保持手段に保持させる生成手段と、前記鍵情報復号手段により得られた鍵情報がコンテンツ鍵を復号するための復号鍵であるとき、秘密鍵暗号方式により暗号化された暗号化コンテンツ鍵を取得し、前記復号鍵を用いて復号してコンテンツ鍵を得て、スクランブル暗号方式によりスクランブルされたコンテンツを取得し、前記コンテンツ鍵を用いてデスクランブルしてコンテンツを再生するコンテンツ再生手段とを備えることを特徴とする。

【０１１４】

上記構成によれば、再生装置は、鍵情報を取得し、鍵情報が鍵更新情報であるとき新たな秘密鍵を生成し、鍵情報が復号鍵であるとき当該復号鍵を用いてコンテンツの再生を行う。このように、鍵更新情報に基づいて新たな秘密鍵を生成することで、次回から新たな秘密鍵により暗号化された鍵情報を適正に復号することができる。

【０１１５】

したがって、秘密鍵の更新後は、正当な再生装置のみがコンテンツを再生でき、不正な再生装置によるコンテンツの再生を排除することができる。

また、前記鍵情報には、鍵更新情報であることを示す識別子又は復号鍵であることを示す識別子が付加されており、前記再生装置は、さらに、前記鍵情報復号手段により得られた鍵情報が、鍵更新情報であるか復号鍵であるかを識別子に基づいて判定する判定手段を備えることとしてもよい。

【０１１６】

上記構成によれば、再生装置は、鍵情報が鍵更新情報であるか復号鍵であるか識別子により識別することができる。

また、前記鍵情報は、ＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｍａｎａｇｅｍｅｎｔ Ｍｅｓｓａｇｅｓ）に含まれており、前記再生装置は、さらに、前記秘密鍵により暗号化されたＥＭＭを含む放送データを受信し、暗号化された鍵情報を得る放送受信手段を備え、前記鍵情報復号手段は、前記放送受信手段により得られる暗号化された鍵情報を取得することとしてもよい。

【０１１７】

秘密鍵の更新方式として、秘密鍵の管理者が正当なユーザに新たな秘密鍵が記録された可搬メディアを送付するなどの方式も考えられる。しかし、その方式は、正当なユーザが可搬メディアを受け取るまでに相当の日数を要し、その間、ユーザがコンテンツを視聴することができないなどの不利益を被る可能性がある。また、秘密鍵の管理者からの視点で言えば、複数の再生装置の秘密鍵を更新するときに、可搬メディアを複数のユーザに個別に送付しなければならず、費用負担が大きい。

【０１１８】

ところが、上記構成によれば、再生装置は、鍵更新情報を放送の受信により取得することができる。鍵更新情報が放送により送信されるため秘密鍵の更新が瞬時に行われる。

したがって、正当なユーザは、上記のような不利益を被ることがない。
また、鍵更新情報が放送により送信されるため秘密鍵の更新が一度に複数の再生装置に通知される。
【０１１９】
したがって、秘密鍵の管理者は、上記のような費用負担を軽減することができる。
また、前記生成手段は、さらに、再生装置毎、再生装置の生産ロット毎、再生装置の機種毎又は再生装置のメーカ毎に異なる所定の変換に基づいて新たな秘密鍵を生成することとしてもよい。
【０１２０】
上記構成によれば、秘密鍵は、再生装置毎、再生装置の生産ロット毎、再生装置の機種毎又は再生装置のメーカ毎に異なる所定の変換に基づいて更新される。
これにより、再生装置がリバースエンジニアリングにより不正に解析され、秘密鍵の変換方式が漏洩したとしても、対策の対象となる再生装置が絞られる。
また、前記鍵更新情報は、新たな秘密鍵の元となるシード情報を含み、前記生成手段は、前記シード情報に所定の変換を施して新たな秘密鍵を生成することとしてもよい。
【０１２１】
上記構成によれば、鍵更新情報は、シード情報を含む。
したがって、再生装置は、シード情報を取得し、そのシード情報に所定の変換を施すだけで新たな秘密鍵を取得することができる。
また、前記鍵更新情報は、秘密鍵の更新を指示するトリガ情報であり、前記生成手段は、さらに、前記トリガ情報に応じて前記秘密鍵を管理する鍵管理装置に秘密鍵の元となるシード情報の取得要求信号を送信する送信手段と、前記取得要求信号に応じて前記鍵管理装置が送信するシード情報を受信するシード情報受信手段とを備え、前記生成手段は、前記シード情報受信手段により受信されたシード情報に所定の変換を施して新たな秘密鍵を生成することとしてもよい。
【０１２２】
上記構成によれば、再生装置は、トリガ情報を取得して、そのトリガ情報により秘密鍵を更新すべきことを知る。その後、再生装置は、鍵管理装置にシード情報の取得を要求してシード情報を受信し、そのシード情報に所定の変換を施すことで新たな秘密鍵を取得することができる。
このように、鍵更新情報を受信した後に鍵管理装置と通信することは、次の２つの利点がある。
【０１２３】
一方は、鍵管理装置が、不正な再生装置の元となった再生装置を特定することができることである。
例えば、再生装置のＩＤを取得要求信号として送信する仕様であれば、不正な再生装置が存在した場合、鍵管理装置には、同一のＩＤが複数回送信されてくることになる。これにより、鍵管理装置は、そのＩＤの再生装置が不正な再生装置の元となったと判断することができる。
【０１２４】
他方は、再生装置がマスタ鍵の更新処理を行っていることを鍵管理装置が知りえることである。例えば、単にシード情報を放送により送信するだけであれば、鍵管理装置は再生装置がマスタ鍵を更新していることを知ることができない。ところが、上記構成によれば、再生装置から通信が行われるので、鍵管理装置は少なくとも再生装置が鍵更新情報を受信したことを認定することができる。
【０１２５】
また、前記鍵更新情報は、新たな秘密鍵の元となるシード情報を含み、前記生成手段は、さらに、１回又は複数回ごとに異なるイベント情報を出力する出力手段を備え、前記生成手段は、所定の変換により、前記シード情報及び前記イベント情報に基づいて新たな秘密鍵を生成し、前記再生装置は、さらに、前記出力手段により出力された前記イベント情報

を前記秘密鍵を管理する鍵管理装置に送信する送信手段を備えることとしてもよい。
【０１２６】
上記構成によれば、再生装置は、シード情報とイベント情報とから新たな秘密鍵を生成する。また、鍵管理装置と新たな秘密鍵を共有するためイベント情報を送信する。
このように、鍵更新情報を受信した後に鍵管理装置と通信することは、次の２つの利点がある。
【０１２７】
一方は、鍵管理装置が、不正な再生装置の元となった再生装置を特定することができることである。
例えば、再生装置のＩＤを取得要求信号として送信する仕様であれば、不正な再生装置が存在した場合、鍵管理装置には、同一のＩＤが複数回送信されてくることになる。これにより、鍵管理装置は、そのＩＤの再生装置が不正な再生装置の元となったと判断することができる。
【０１２８】
他方は、再生装置がマスタ鍵の更新処理を行っていることを鍵管理装置が知りえることである。例えば、単にシード情報を放送により送信するだけであれば、鍵管理装置は再生装置がマスタ鍵を更新していることを知ることができない。ところが、上記構成によれば、再生装置から通信が行われるので、鍵管理装置は少なくとも再生装置が鍵更新情報を受信したことを認定することができる。
【０１２９】
また、前記保持手段は、再生装置毎、再生装置の生産ロット毎、再生装置の機種毎又は再生装置のメーカ毎に個別の秘密鍵を保持していることとしてもよい。
上記構成によれば、秘密鍵は、再生装置毎、再生装置の生産ロット毎、再生装置の機種毎又は再生装置のメーカ毎に異なる。
これにより、再生装置がリバースエンジニアリングにより不正に解析され、秘密鍵の変換方式が漏洩したとしても、対策の対象となる再生装置が絞られる。
【０１３０】
また、前記再生装置は、再生装置毎、再生装置の生産ロット毎、再生装置の機種毎又は再生装置のメーカ毎に個別のＩＤを有し、前記生成手段は、前記シード情報及び前記ＩＤに所定の変換を施して新たな秘密鍵を生成することとしてもよい。
上記構成によれば、ＩＤは、再生装置毎、再生装置の生産ロット毎、再生装置の機種毎又は再生装置のメーカ毎に異なる。
【０１３１】
これにより、再生装置がリバースエンジニアリングにより不正に解析され、秘密鍵の変換方式が漏洩したとしても、対策の対象となる再生装置が絞られる。
本発明に係る、秘密鍵を保持する保持部を有する再生装置が、コンテンツを再生する再生方法は、秘密鍵暗号方式により暗号化された暗号化鍵情報を取得し、前記秘密鍵を用いて前記暗号化鍵情報を復号して鍵情報を得る鍵情報復号ステップと、前記鍵情報復号ステップにより得られた鍵情報が前記秘密鍵の更新に用いる鍵更新情報であるとき、当該鍵更新情報に基づいて新たな秘密鍵を生成し、前記鍵情報復号ステップにおいて用いる秘密鍵として前記保持部に保持させる生成ステップと、前記鍵情報復号ステップにより得られた鍵情報がコンテンツ鍵を復号するための復号鍵であるとき、秘密鍵暗号方式により暗号化された暗号化コンテンツ鍵を取得し、前記復号鍵を用いて復号してコンテンツ鍵を得て、スクランブル暗号方式によりスクランブルされたコンテンツを取得し、前記コンテンツ鍵を用いてデスクランブルしてコンテンツを再生するコンテンツ再生ステップとを含むことを特徴とする。
【０１３２】
上記構成によれば、再生装置は、鍵情報を取得し、鍵情報が鍵更新情報であるとき新たな秘密鍵を生成し、鍵情報が復号鍵であるとき当該復号鍵を用いてコンテンツの再生を行う。このように、鍵更新情報に基づいて新たな秘密鍵を生成することで、次回から新たな秘

密鍵により暗号化された鍵情報を適正に復号することができる。
【０１３３】
したがって、秘密鍵の更新後は、正当な再生装置のみがコンテンツを再生でき、不正な再生装置によるコンテンツの再生を排除することができる。
本発明に係る、秘密鍵の保持部を有するコンピュータにコンテンツを再生させるプログラムは、秘密鍵暗号方式により暗号化された暗号化鍵情報を取得し、前記秘密鍵を用いて前記暗号化鍵情報を復号して鍵情報を得る鍵情報復号ステップと、前記鍵情報復号ステップにより得られた鍵情報が前記秘密鍵の更新に用いる鍵更新情報であるとき、当該鍵更新情報に基づいて新たな秘密鍵を生成し、前記鍵情報復号ステップにおいて用いる秘密鍵として前記保持部に保持させる生成ステップと、前記鍵情報復号ステップにより得られた鍵情報がコンテンツ鍵を復号するための復号鍵であるとき、秘密鍵暗号方式により暗号化された暗号化コンテンツ鍵を取得し、前記復号鍵を用いて復号してコンテンツ鍵を得て、スクランブル暗号方式によりスクランブルされたコンテンツを取得し、前記コンテンツ鍵を用いてデスクランブルしてコンテンツを再生するコンテンツ再生ステップとを含むことを特徴とする。
【０１３４】
上記構成によれば、コンピュータは、鍵情報を取得し、鍵情報が鍵更新情報であるとき新たな秘密鍵を生成し、鍵情報が復号鍵であるとき当該復号鍵を用いてコンテンツの再生を行う。このように、鍵更新情報に基づいて新たな秘密鍵を生成することで、次回から新たな秘密鍵により暗号化された鍵情報を適正に復号することができる。
【０１３５】
したがって、秘密鍵の更新後は、正当な再生装置のみがコンテンツを再生でき、不正な再生装置によるコンテンツの再生を排除することができる。
本発明に係る、秘密鍵暗号方式における秘密鍵を管理する鍵管理装置は、前記秘密鍵の更新に用いる鍵更新情報を生成する鍵更新情報生成手段と、前記生成手段により生成された鍵更新情報又はコンテンツを再生するための復号鍵を鍵情報とし、当該鍵情報を前記秘密鍵により暗号化して前記再生装置に送信する送信手段と、前記鍵更新情報に基づいて新たな秘密鍵を生成し、前記送信手段において用いられる秘密鍵とする秘密鍵生成手段とを備えることを特徴とする。
【０１３６】
上記構成によれば、鍵管理装置は、暗号化された鍵情報を再生装置に送信する。これにより、鍵管理装置と再生装置とが同じ鍵情報を有することができる。
また、鍵管理装置は、鍵情報に含まれる鍵更新情報により秘密鍵を更新することができる。
したがって、秘密鍵の更新後は、正当な再生装置のみがコンテンツを再生でき、不正な再生装置のコンテンツの再生を排除することができる。
【０１３７】
また、前記送信手段は、さらに、前記鍵情報に、当該鍵情報が鍵更新情報であることを示す識別子又は復号鍵であることを示す識別子を付加して送信することとしてもよい。
上記構成によれば、鍵管理装置は、同じ形式を用いて復号鍵と鍵更新情報との２種類の情報を送信することができる。
【０１３８】
また、前記鍵情報は、ＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｍａｎａｇｅｍｅｎｔ Ｍｅｓｓａｇｅｓ）に含まれており、前記送信手段は、前記鍵情報を放送により再生装置に送信することとしてもよい。
上記構成によれば、鍵管理装置は、鍵更新情報を放送により送信することができる。鍵更新情報が放送により送信されるため秘密鍵の更新が瞬時に行われる。
【０１３９】
また、前記鍵更新情報は、新たな秘密鍵の元となるシード情報を含み、前記秘密鍵生成手段は、前記シード情報に所定の変換を施して新たな秘密鍵を生成することとしてもよい。

上記構成によれば、鍵更新情報は、シード情報を含む。
したがって、鍵管理装置は、シード情報を生成し、そのシード情報に所定の変換を施すだけで新たな秘密鍵を取得することができる。
【０１４０】
また、前記鍵更新情報は、秘密鍵の更新を指示するトリガ情報であり、前記秘密鍵生成手段は、さらに、新たな秘密鍵の元となるシード情報を生成するシード情報生成手段と、前記トリガ情報を取得した再生装置から送信される取得要求信号を受信し、当該取得要求信号に応じて、前記シード情報生成手段により生成されたシード情報を前記再生装置に伝送する伝送手段とを含み、前記秘密鍵生成手段は、前記シード情報に所定の変換を施して新たな秘密鍵を生成することとしてもよい。
【０１４１】
上記構成によれば、鍵管理装置は、トリガ情報を生成して、そのトリガ情報により再生装置に秘密鍵を更新すべきことを通知する。その後、再生装置からのシード情報の取得要求信号を受信し、それに応じてシード情報を再生装置に送信する。また、シード情報に所定の変換を施すことで新たな秘密鍵を取得することができる。
【０１４２】
このように、鍵更新情報を送信した後に鍵管理装置と通信することは、次の２つの利点がある。
一方は、鍵管理装置が、不正な再生装置の元となった再生装置を特定することができることである。
例えば、再生装置のＩＤを取得要求信号として送信する仕様であれば、不正な再生装置が存在した場合、鍵管理装置には、同一のＩＤが複数回送信されてくることになる。これにより、鍵管理装置は、そのＩＤの再生装置が不正な再生装置の元となったと判断することができる。
【０１４３】
他方は、再生装置がマスタ鍵の更新処理を行っていることを鍵管理装置が知りえることである。例えば、単にシード情報を放送により送信するだけであれば、鍵管理装置は再生装置がマスタ鍵を更新していることを知ることができない。ところが、上記構成によれば、再生装置から通信が行われるので、鍵管理装置は少なくとも再生装置が鍵更新情報を受信したことを認定することができる。
【０１４４】
また、前記鍵更新情報は、新たな秘密鍵の元となるシード情報を含み、前記秘密鍵生成手段は、さらに、前記シード情報を取得した再生装置から送信される１回又は複数回ごとに異なるイベント情報を受信する受信手段を含み、前記秘密鍵生成手段は、所定の変換により、前記シード情報及び前記イベント情報に基づいて新たな秘密鍵を生成することとしてもよい。
【０１４５】
上記構成によれば、鍵管理装置は、イベント情報を再生装置から受信し、シード情報とイベント情報とから新たな秘密鍵を生成する。
このように、鍵更新情報を受信した後に鍵管理装置と通信することは、次の２つの利点がある。
一方は、鍵管理装置が、不正な再生装置の元となった再生装置を特定することができることである。
【０１４６】
例えば、再生装置のＩＤを取得要求信号として送信する仕様であれば、不正な再生装置が存在した場合、鍵管理装置には、同一のＩＤが複数回送信されてくることになる。これにより、鍵管理装置は、そのＩＤの再生装置が不正な再生装置の元となったと判断することができる。
他方は、再生装置がマスタ鍵の更新処理を行っていることを鍵管理装置が知りえることである。例えば、単にシード情報を放送により送信するだけであれば、鍵管理装置は再生装

置がマスタ鍵を更新していることを知ることができない。ところが、上記構成によれば、再生装置から通信が行われるので、鍵管理装置は少なくとも再生装置が鍵更新情報を受信したことを認定することができる。

【０１４７】

本発明に係る、コンテンツを再生する再生装置と、当該再生装置の秘密鍵暗号方式における秘密鍵を管理する鍵管理装置からなる鍵管理システムは、鍵管理装置において、前記秘密鍵の更新に用いる鍵更新情報を生成する鍵更新情報生成手段と、前記鍵更新情報生成手段により生成された鍵更新情報又はコンテンツを再生するための復号鍵を鍵情報とし、当該鍵情報を前記秘密鍵により暗号化して前記再生装置に送信する送信手段と、前記再生装置において、前記送信手段により送信される暗号化鍵情報を取得し、保持している秘密鍵を用いて当該暗号化鍵情報を復号して前記鍵情報を得る鍵情報復号手段と、前記鍵管理装置において、前記鍵更新情報に基づいて新たな秘密鍵を生成し、前記送信手段において用いる秘密鍵とする第１生成手段と、前記再生装置において、前記鍵情報復号手段により復号された鍵情報が鍵更新情報であるとき、前記鍵更新情報に基づいて新たな秘密鍵を生成し、前記鍵情報復号手段において用いる秘密鍵とする第２生成手段とを備えることを特徴とする。

【０１４８】

上記構成によれば、再生装置及び鍵管理装置は、鍵情報を取得し、鍵情報が鍵更新情報であるとき秘密鍵を更新し、鍵情報が復号鍵であるとき当該復号鍵を用いてコンテンツの再生を行う。このように、鍵更新情報により秘密鍵を更新することで、次回から新たな秘密鍵により暗号化された鍵情報を適正に復号することができる。

【０１４９】

したがって、秘密鍵の更新後は、正当な再生装置のみがコンテンツを再生でき、不正な再生装置のコンテンツの再生を排除することができる。

【図面の簡単な説明】

【図１】限定受信システムの概略を示す図である。

【図２】限定受信システムにおける再生装置の構成を示す図である。

【図３】限定受信システムにおける再生装置の動作を示す図である。

【図４】複数の再生装置における限定受信システムの概略を示す図である。

【図５】限定受信システムにおける複数の再生装置の動作を示す図である。

【図６】不正再生装置が存在する場合の限定受信システムの概略を示す図である。

【図７】不正再生装置によるコンテンツの不正な再生を阻止する場合の各再生装置の動作を示す図である。

【図８】実施の形態１における限定受信システムの概要を示す図である。

【図９】限定受信システムにおける再生装置の構成を示す図である。

【図１０】実施の形態１におけるＫｍ更新部の詳細な構成を示す図である。

【図１１】通常のＥＭＭのデータ構造を示す図である。

【図１２】マスタ鍵Ｋｍの更新のためのＥＭＭのデータ構造を示す図である。

【図１３】Ｋｍ生成部におけるアルゴリズムの例を示す図である。

【図１４】限定受信システムにおける再生装置の動作を示す図である。

【図１５】限定受信システムにおける鍵管理装置の構成を示す図である。

【図１６】鍵管理装置におけるＩＤとマスタ鍵Ｋｍとの管理例を示す。

【図１７】限定受信システムにおける鍵管理装置の動作を示す図である。

【図１８】不正再生装置によるコンテンツの不正な視聴を排除するときの各再生装置の動作を示す図である。

【図１９】実施の形態２における限定受信システムの概要を示す図である。

【図２０】実施の形態２におけるＫｍ更新部の詳細な構成を示す図である。

【図２１】マスタ鍵Ｋｍの更新のためのＥＭＭのデータ構造を示す図である。

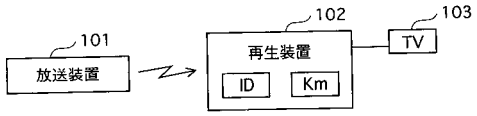
【図２２】限定受信システムにおける鍵管理装置の構成を示す図である。

【図２３】実施の形態３における限定受信システムの概要を示す図である。

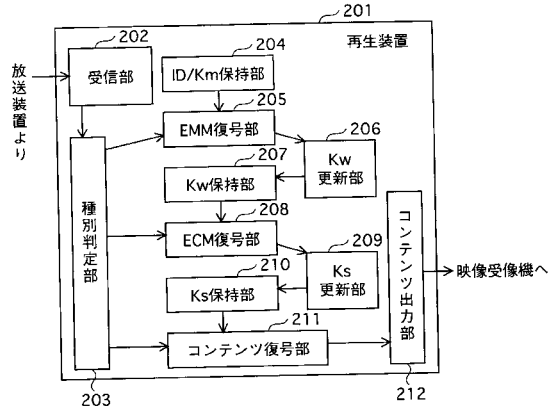
【図２４】実施の形態３におけるＫｍ更新部の詳細な構成を示す図である。
【図２５】限定受信システムにおける鍵管理装置の構成を示す図である。
【図２６】ＤＶＤの再生装置の構成を示す図である。
【符号の説明】
９０１　再生装置
９０２　受信部
９０３　種別判定部
９０４　ＩＤ／Ｋｍ保持部
９０５　ＥＭＭ復号部
９０６　更新情報判定部
９０７　Ｋｗ更新部
９０８　Ｋｗ保持部
９０９　ＥＣＭ復号部
９１０　Ｋｓ更新部
９１１　Ｋｓ保持部
９１２　コンテンツ復号部
９１３　コンテンツ出力部
９１４　Ｋｍ更新部
１００１　シード情報取得部
１００２　Ｋｍ生成部
１００３　Ｋｍ保存部
１５０１　鍵管理装置
１５０２　ＥＭＭ受信部
１５０３　鍵更新判定部
１５０４　シード情報生成挿入部
１５０５　Ｋｍ更新部
１５０６　ＩＤ／Ｋｍ保持部
１５０７　ＥＭＭ暗号部
１５０８　暗号化ＥＭＭ送信部
２００１　装置情報保持部
２００２　装置情報送信部
２００３　シード情報受信部
２００４　Ｋｍ生成部
２００５　Ｋｍ保存部
２２０１　鍵管理装置
２２０２　ＥＭＭ受信部
２２０３　鍵更新判定部
２２０４　シード情報生成部
２２０５　Ｋｍ更新部
２２０６　ＩＤ／Ｋｍ保持部
２２０７　ＥＭＭ暗号部
２２０８　暗号化ＥＭＭ送信部
２２０９　装置情報受信部
２２１０　シード情報送信部
２４０１　シード情報取得部
２４０２　装置情報生成部
２４０３　Ｋｍ生成部
２４０４　Ｋｍ保存部
２４０５　装置情報送信部
２５０４　シード情報生成挿入部

２５０５　　装置情報受信部
２５０６　　Ｋｍ更新部

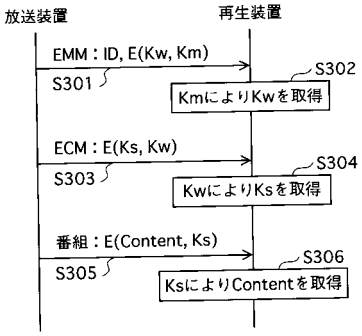
【図１】



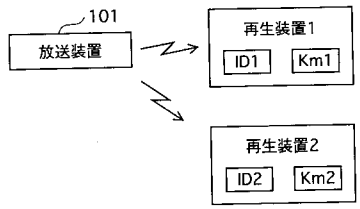
【図２】



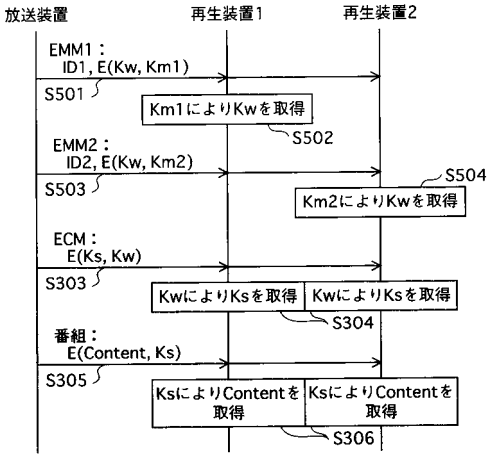
【図３】



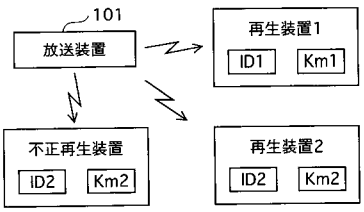
【図４】


101
放送装置
再生装置1
ID1
Km1
再生装置2
ID2
Km2

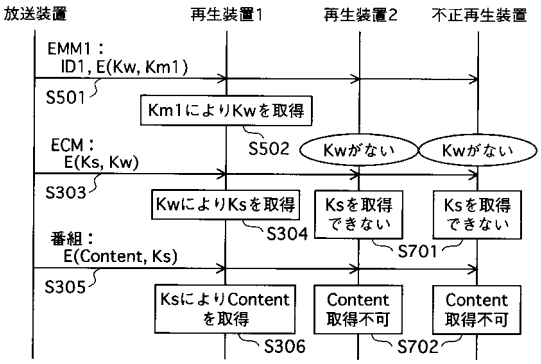
【図５】


放送装置
再生装置1
再生装置2
EMM1：
ID1, E(Kw, Km1)
S501
Km1によりKwを取得
S502
EMM2：
ID2, E(Kw, Km2)
S503
S504
Km2によりKwを取得
ECM：
E(Ks, Kw)
S303
KwによりKsを取得
KwによりKsを取得
S304
番組：
E(Content, Ks)
S305
KsによりContentを取得
KsによりContentを取得
S306

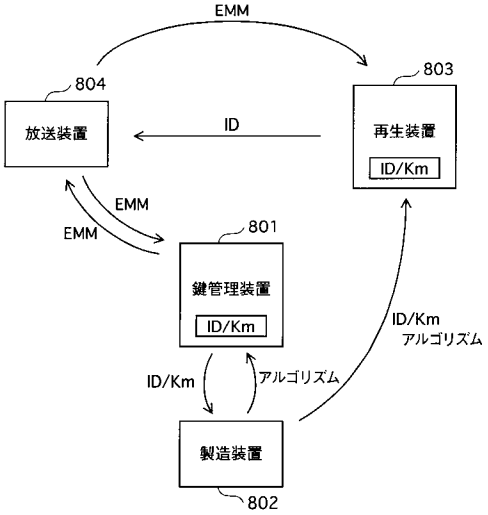
【図６】


101
放送装置
再生装置1
ID1
Km1
不正再生装置
ID2
Km2
再生装置2
ID2
Km2

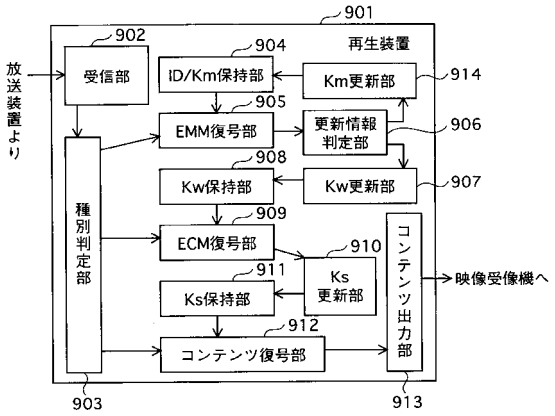
【図７】


放送装置
再生装置1
再生装置2
不正再生装置
EMM1：
ID1, E(Kw, Km1)
S501
Km1によりKwを取得
S502
Kwがない
Kwがない
ECM：
E(Ks, Kw)
S303
KwによりKsを取得
S304
Ksを取得できない
Ksを取得できない
S701
番組：
E(Content, Ks)
S305
KsによりContentを取得
Content取得不可
Content取得不可
S306
S702

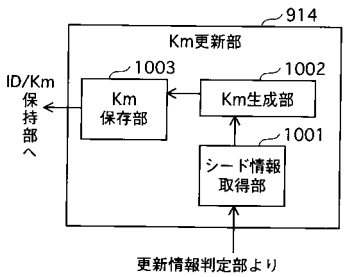
【図８】



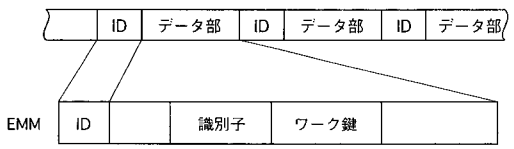
【図９】



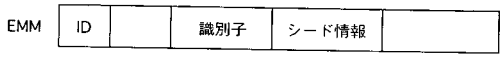
【図１０】



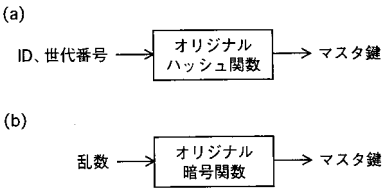
【図１１】



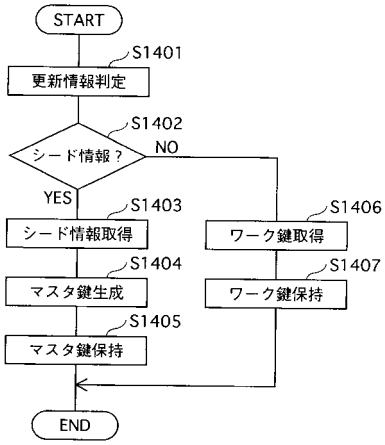
【図１２】



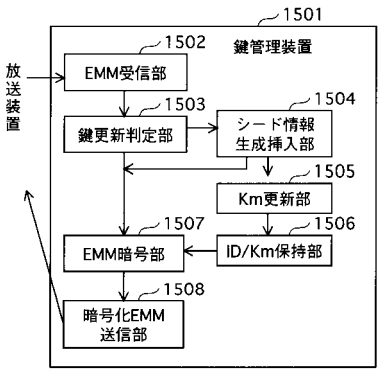
【図１３】



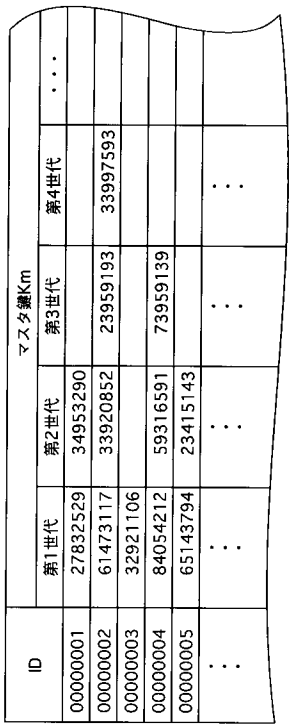
【図１４】



【図１５】

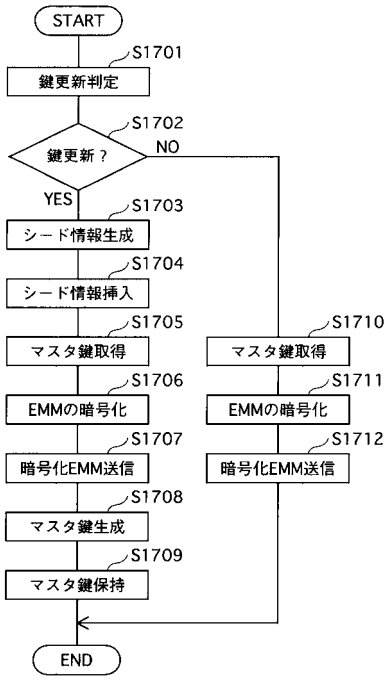


【図１６】

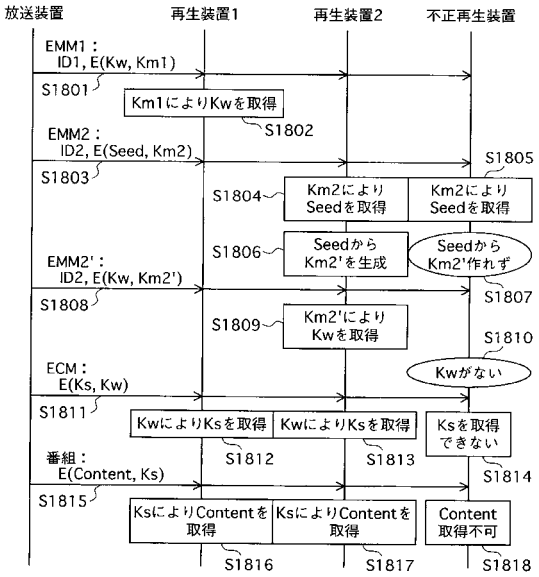


ID	マスタ鍵Km 第1世代	第2世代	第3世代	第4世代	・・・
00000001	27832529	34953290		33997593	・・・
00000002	61473117	33920852	23959193		・・・
00000003	32921106				
00000004	84054212	59316591	73959139		・・・
00000005	65143794	23415143			・・・
・・・					

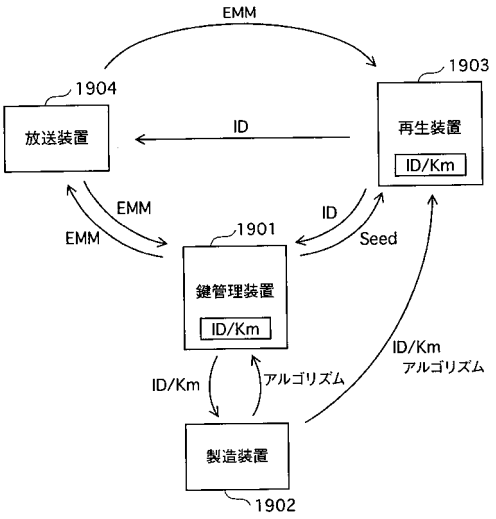
【図１７】



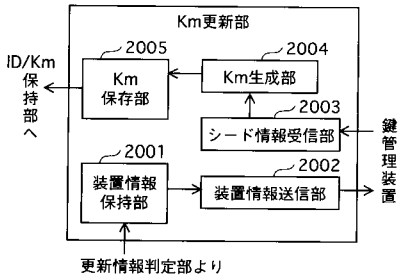
【図１８】



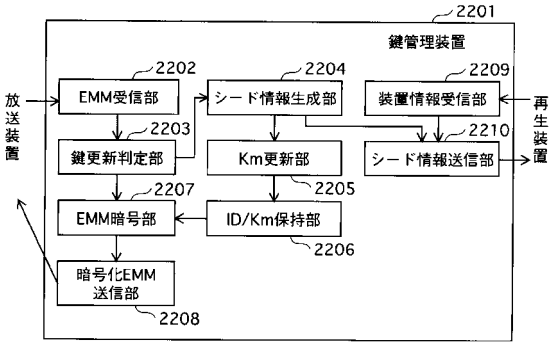
【図１９】



【図２０】

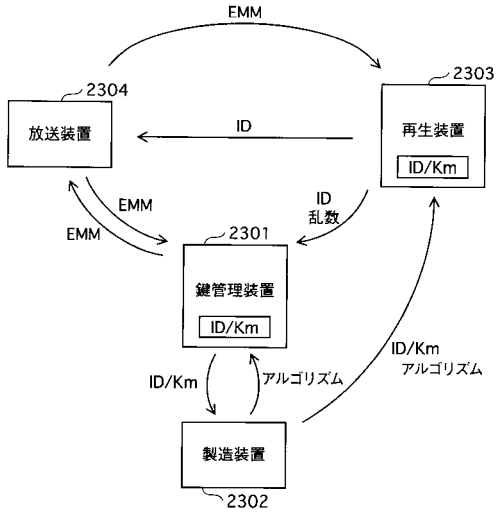


【図２２】

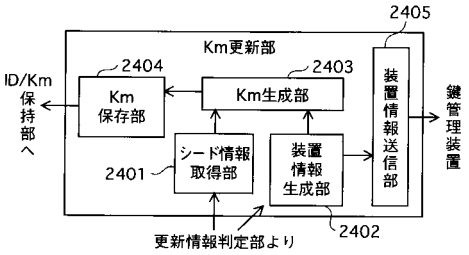


【図２１】

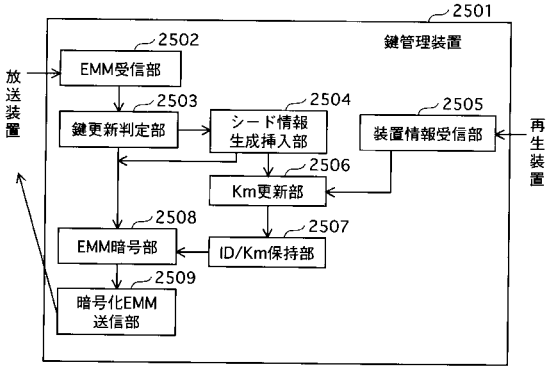
【図２３】



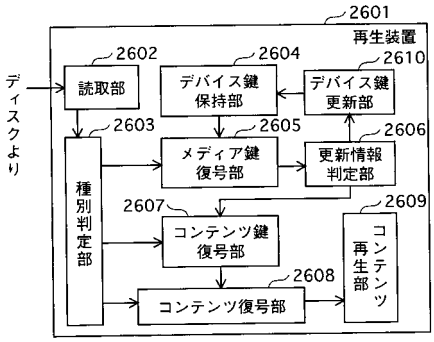
【図２４】



【図２５】



【図２６】



フロントページの続き

(72)発明者　山田　茂
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　村上　弘規
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　井上　哲也
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　大森　基司
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

Ｆターム(参考) 5J104 EA23　JA03　PA14